



Central Bank of India

Request for Proposal (Bid) Document

For

RFP for “Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels”

Bid Number: GEM/2026/B/7384926

24th March 2026

Contents

Table of Contents

1.	List of Abbreviations	7
2.	Overview and Objectives	11
3.	Invitation to BID	12
4.	Bidding Process	12
5.	Definitions.....	13
6.	Disclaimer.....	14
7.	Instructions to Bidders:.....	15
7.1	Pre Bid Meeting.....	15
7.2	Amendment of bidding document.....	16
7.3	Technical Bid	16
7.4	Commercial Bid	16
7.5	Bid Security (EMD).....	16
7.6	Performance Bank Guarantee (PBG).....	16
8.	Eligibility & Evaluation Criteria	18
8.1	Eligibility Criteria	18
8.2	Stages of Evaluation	21
A.	Eligibility Criteria Evaluation:.....	21
B.	Technical Evaluation	21
C.	Evaluation of Technical Competence:	22
D.	Presentation and Demo.....	25
9.	Commercial Evaluation	25
10.	SCOPE OF WORK.....	29
A.	Functional Scope of Work:.....	29
B.	Technical Scope of Work:.....	57
11.	Software License	72
12.	Hardware Requirement	75
13.	Onsite Support:	77
14.	Training.....	79
15.	Important General Terms & Conditions	80
15.1.	Maintenance Support:	80

15.2.	ESCROW Arrangement:	80
15.3.	Compliance with Laws:	81
15.4	Compliance in obtaining approvals/permissions/licenses:	81
15.5	Right to Alter:	81
15.5	Conflict of Interest:	81
15.6	Information Ownership:	81
15.7	Liquidated damages:	82
15.8	Land Border Sharing Clause:	82
15.9	Monitoring & Audit:	83
15.10	Bid Submission:	84
15.11	Integrity Pact:	84
15.12	Commercial Offers:	85
15.13	Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)	87
15.14	Payment Terms	87
15.15	Terms & Conditions:	90
15.16	Intellectual Property	91
15.17	Enterprise Licensing	92
15.18	Facility Management and Maintenance Services	93
15.19	Mandatory Training/Knowledge Transfer	99
15.20	Service Level Agreement	100
15.21	Implementation Schedule	108
	Annexure 1: Conformity Letter:	123
	Annexure 2: Compliance to Terms & Conditions	124
	Annexure 3: Pro-forma for deed of indemnity: *	125
	Annexure 4: Undertaking of Authenticity for Products Supplied:	127
	Annexure 5: Undertaking for Acceptance of Terms of RFP	128
	Annexure 6: Manufacturer's / OSD Authorization Form:	129
	Annexure 7: Pre- Contract Integrity Pact	130
	Annexure 8: Non-Disclosure Agreement:	136
	Annexure 9: Performance Bank Guarantee (PBG):	141
	Annexure 10: Pro-forma for Bid Security (EMD):	144
	Annexure 11: Letter for Refund of EMD:	146
	Annexure 12: NPA Undertaking:	147
	Annexure 13: Undertaking letter - Land Border Sharing:	148

Annexure 14: List of Hardware and Software Components:	151
Annexure 15: Cover Letter:.....	153
Annexure 16: Bidder’s Particulars on Company Letter Head:	154
Annexure 17: Guidelines on banning of business dealing:.....	156
Annexure 18: Proposed Team Profile:	158
Annexure 19: Format for Submission of Client References by Bidder.	159
Annexure 20: Query Format:	161
Annexure 21: Eligibility Criteria Compliance:	162
Annexure 22: Undertaking for 5 Year Roadmap:.....	167
Annexure 23: Compliance to Security Control:.....	168
Annexure 24: Undertaking for Information Security:	177
Annexure 25: Undertaking for Data Privacy:.....	178
Annexure 26: Format for Local Content : (Make in India)	179
Annexure 27: Undertaking for Non- Blacklisting/ Non-Debarment of the bidder	180
Annexure 28: Masked Commercial Bid.....	182
Annexure 29: Functional Specifications	190
Annexure 30: Technical Specifications.....	207
Annexure 31: Board Resolution	227
Annexure 32: Format for Submission of Client References by Bidder.	229
16. Checklist For Submission:	230

IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION

TABLE-1		
S. No	Particulars	Timeline
1	Tender Reference	Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels
2	Date of RFP Issuance	24/03/2026
3	Last Date of Receiving request for queries / clarifications before the Pre-bid Meeting	02/04/2026
4	Bid Security (EMD)	An amount of ₹40,00,000/- (Rupees Forty Lakhs Only) in the form of Bank Guarantee issued by a scheduled commercial bank other than Central Bank of India for the entire non-interest bearing period of Bid validity of 180 days plus 3 months or by means of banker's cheque/ Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration “Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels” in favor of “Central Bank of India” and payable at Mumbai/Navi Mumbai.
5	Pre-bid Meeting Date and Venue Details	06/04/2026 at 03:00 PM Central Bank of India Cent Neo, 6th Floor, Tower No.7 Belapur Railway Station Complex, Sector-11, CBD Belapur, Navi Mumbai- 400614
6	Last Date and Time for submission of Bids, Mode of bid submission & online portal's URL	24/04/2026 up to 15:00 hrs. Mode-Online through GeM
7	Time & Date of Opening of technical bids	24/04/2026 online at 15:30 hrs.
8	Date, time and venue of presentation & demo by the eligible bidders	Shall be intimated separately by the Bank through email to the eligible bidders.

9	Opening of commercial bids	Date and time will be intimated to technically qualified bidders by email registered during bid submission.
10	Address for Communication	Asst. General Manager - IT, Central Bank of India Cent Neo, 6th Floor, Tower No.7 Belapur Railway Station Complex, Sector-11, CBD Belapur, Navi Mumbai- 400614 <u>Email address:</u> agmitneo@centralbank.co.in cmneoliab@centralbank.co.in cmneoliab1@centralbank.co.in
11	Contact Numbers	+91-6303929016 +91-9080315326 +91-898961267

1. List of Abbreviations

The long form of some abbreviations commonly used in the bid is given below:

Abbreviations	Description
AI/ML	Artificial Intelligence/Machine Learning
AMC	Annual Maintenance Contract
API	Application Programming Interface
ATS	Annual Technical Services
BG	Bank Guarantee
BOD	Beginning of Day
BOM	Bill of Material
CBS	Core Banking Solutions
CBoI	Central Bank of India
CC	Cash Credit
CIF	Customer Identification File/Form
CRM	Customer Relationship Management
CSV	Comma-Separated Value
CVC	Central Vigilance Commission
DC	Data Center
DKYC	Digital Know Your Customer
DDOS	Distributed Denial-of-Service
DIT	Department of Information Technology
DR	Disaster Recovery
EFRM	Enterprise Fraud Risk Management
EMD	Earnest Money Deposit
EOD	End of Day
EOL	End of Life
EOS	End of Support/Sale
ERP	Enterprise Resource Planning



EWS	Early Warning System
FAQ's	Frequently Asked Questions
FI	Financial Institute
FMS	Facility Management Services
FTP	File Transfer Protocol
GB	Giga Byte
GFR	General Financial Rules
GST	Goods and Service Tax
GSTIN	Goods and Service Tax Identification Number
GUI	Graphical User Interface
H2H	Host to Host
HO	Head Office
HTML	Hyper Text Markup Language
IB/INB	Internet Banking
IBA	Indian Bank's Association
ICC	Integrated Customer Care
IPO	Initial Public Offering
IPC (BNS)	Indian Penal Code (Bharatiya Nyaya Sanhita)
PCA	Prevention of Corruption Act
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
KYC	Know Your Customer
KRI	Key Risk Indicator
LAPS	Lending Automation of Processing System
LEI	Legal Entity Identifier
LD	Liquidated Damage
LMS	Loan Management System



LOI	Letter of Intent
LOS	Loan Origination System
MB	Mobile Banking
MIS	Management Information System
MICR	Magnetic Ink Character Recognition
ML	Machine Learning
MSE	Micro & Small Enterprise
MSME	Micro, Small & Medium Enterprises
MT	Message Type
NBFC	Non-Banking Financial Company
NDA	Non-Disclosure Agreement
NEFT	National Electronic Funds Transfer
NI Act	Negotiable Instruments Act
NPA	Non-Performing Asset
NPCI	National Payments Corporation of India
OCR	Optical Character Recognition
OD	Overdraft
OEM	Original Equipment Manufacturer
OSD	Original Solution Developer
P&L	Profit and Loss
PAN	Permanent Account Number
PAT	Profit After Tax
PAO	Pay and Accounts Office
PBG	Performance Bank Guarantee
PGP	Pretty Good Privacy
PO	Purchase Order
PoA	Power of Attorney
POC	Proof Of Concept



QR	Quick Response
RAM	Random Access Memory
RFP	Request for Proposal
RBI	Reserve Bank of India
RO	Regional Office
RPA	Robotic Process Automation
RPO	Recovery Point Objective
RRN	Retrieval Reference Number
RTGS	Real Time Gross Settlement
RTO	Recovery Time Objective
SAN	Unique Short Account Number/ Storage area Network
SAP	System Application
SB	Successful Bidder
SCB's	Scheduled Commercial Bank's
SEBI	Security and Exchange Board of India
SFTP	Secure File Transfer Protocol
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMS	Short Message Service
SP	Service Provider
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign On
STP	Straight Through Processing
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAN	Tax Deduction and Collection Account Number
TAT	Turn Around Time
TCO	Total Cost of Ownership

TSP	Technology Service Provider
UAT	User Acceptance Testing
UDIN	Unique Document Identification Number
UIN	Unique Identification Number
UPI	Unified Payments Interface
UTM	Urchin Tracking Module
UTR	Unique Transaction Reference
VAPT	Vulnerability Assessment and Penetration Testing
VM	Virtual Machines
VKYC	Video Know Your Customer
V-CIP	Video base Customer Identification Process
WAF	Web Application Firewall
XML	Extensible Markup Language
ZO	Zonal Office

2. Overview and Objectives

To implement a secure, compliant, Agile driven, AI-powered, scalable and Omni-channel Video-CIP/Digital KYC platform that enables seamless end-to-end digital customer onboarding through an on-premises solution.

For this Bank intends to On-board an additional vendor for developing, installing, configuring, customizing, integrating, implementing, supplying and maintaining of DIGITAL KYC and VIDEO KYC Solutions as per the requirement of the Bank. As this shall be an additional setup parallel to the existing setup, hence the incumbent vendor is not permitted to participate in the RFP process. The bidders cannot propose an incumbent solution in response to this RFP.

In this regard, Central Bank of India invites tenders comprising of eligibility, technical bid and Commercial bid from experienced bidders having proven capabilities of providing DIGITAL KYC and VIDEO KYC Solutions. The prospective bidders are required to adhere to the terms of this RFP document and any deviations to the same shall not be acceptable to the Bank.

The bidder (also called the vendor or bidder through this document) appointed under this RFP document shall own the single point responsibility for fulfilling all obligations

and providing all deliverables and services required for successful implementation of the project. Unless agreed specifically by the Bank in writing for any changes in the document issued, the bidder's responses should comply with the scope of work.

3. Invitation to BID

Central Bank of India, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chander Mukhi, Nariman Point, Mumbai-400021 hereinafter called "Bank" and having 90 Regional Offices (ROs), 14 Zonal Offices (ZOs) and 4600 plus branches spread across India, invites online tender offers (Technical offer and Commercial offer) as Bank intends to on-board a vendor for developing, installing, configuring, customizing, integrating, implementing, supplying and maintaining of DIGITAL KYC and VIDEO KYC Solutions as per the requirement of the Bank.

- 3.1 Bidder shall mean any legal entity who meets the eligibility criteria given in this RFP and willing to provide the Software Solution/ service as required in this RFP. The interested Bidders who agree to all the terms and conditions contained in this RFP may submit their Bids as per terms and conditions in this RFP. Consortium bidding is not permitted under this RFP.
- 3.2 Address for submission of online Bids, contact details including email address for sending communications are given in Table-1 of this RFP.
- 3.3 The purpose of the Bank behind this RFP is to seek a detailed technical and commercial proposal for procurement of the Software Solution desired in this RFP. The proposed Software Solution must integrate with Bank's existing infrastructure seamlessly.
- 3.4 This RFP document shall not be transferred, reproduced or otherwise used for purpose other than for which it is specifically issued.
- 3.5 Interested Bidders are advised to go through and understand the entire RFP before submission of online Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for supply of proposed Software Solution/ service for the Bank are invited to submit their technical and commercial proposal in response to this RFP.
- 3.6 The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at Bank's discretion.
- 3.7 This RFP seeks proposal from Bidders who have the necessary experience, capability & expertise to provide the Bank, the proposed Software Solution/ service adhering to Bank's requirements outlined in this RFP.

4. Bidding Process

A complete set of tender documents may be downloaded by prospective bidders from the Bank's Website.

Bidder should satisfy all the requisite eligibility criteria mentioned in this RFP document.

Bids must be submitted online only through GeM portal. The bidders should also submit necessary documents physically through offline mode to the address mentioned in the RFP.

The Commercial Bid will be submitted online through GeM portal only and intimation will be given by email to all qualifying bidders about the date and time of opening of commercial bids.

The pre bid meeting will be held in person with the bidders as per the stipulated time and at the venue mentioned in the RFP document.

For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs as per the prescribed format by email to the Bank. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only as per Annexure-20 and should be sent to email IDs within stipulated time as mentioned in Table-1.

In accordance with Government of India guidelines, Micro and Small Enterprises are exempted from payment of earnest money deposit upon submission of valid MSE certificate copy.

Start-ups (which are not MSEs) are exempted from Bid security (EMD) amount. Tender offers will normally be opened half an hour after the closing time.

Functional and Technical Specifications, Terms and Conditions and various formats and proforma for submitting the tender offer are described in the tender document and its Annexures.

5. Definitions

In this connection, the following terms shall be interpreted as indicated below:

5.1 "The Bank" means the Central Bank of India (including Branches, Regional Offices, Zonal Offices and Corporate Office, Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures.

5.2 "Bidder/Channel Partner" means an eligible entity/firm submitting the Bid in response to this RFP.

5.3 "Bid" means the written reply or submission of response to this RFP.

5.4 "The Contract" means the agreement entered between the Bank and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

5.5 "Total Contract Price/Project Cost/TCO" means the price payable to Service Provider over the entire period of Contract for the full and proper performance of its contractual obligations.

5.6 "Vendor/Service Provider" is the successful Bidder found eligible as per eligibility criteria set out in this RFP, whose technical Bid has been accepted and who has emerged as successful Bidder as per the selection criteria set out in the RFP and to whom

notification of award has been given by the Bank

5.7 "RFP"- Request for Proposal for the selection of Service Provider for developing, installing, configuring, customizing, integrating, implementing, supplying and maintaining of DIGITAL KYC and VIDEO KYC Solutions as per the requirement of the Bank and which also include the amended/ clarified bidding documents as mentioned in clause 7. (B.) of this RFP and which Bank publishes on the Bank's website and GeM portal as well at any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification(s) requested by a prospective Bidder, may modify/ cancel/ extend/ amend the Bidding Document by modification(s) / amendment(s).

5.8 "Technology Solution/ Services/ System/ Platform" means all software products, services, infrastructure, equipment/products, scope of work and deliverables to be provided by a Bidder along with OEM as described in the RFP and include services ancillary to the development of the solution, such as installation, commissioning, integration with existing systems, provision of technical assistance, knowledge transfer, reporting and other obligation of Service Provider covered under the RFP. The integration should be made with minimal customization in existing system.

5.9 "Annual Maintenance Contract (AMC) / Annual Technical Support (ATS)" - It would cover comprehensive onsite support for the proposed Solution, Infrastructure and Services during the contract period.

5.10 "The Equipment/Product" means all the hardware, it's all components, associated software/firmware/operating software which the Service Provider is required to supply to the Bank as part of the scope of the RFP.

5.11 "Communication channels" means the mode of communication with the customers, internal and external stakeholders like email, SMS, WhatsApp, Chatbots (text and voice), Integrated Customer Care and any other channel which Bank may mandate the vendor to integrate from time to time during the contract period.

5.12 "Bank's Source Systems" means the systems including but not limited to Core Banking System, Corporate Website, Internet Banking, Mobile Banking, UPI System, Payment Middleware, Payment Hub, Omni Channel, CRM, Data Lake, Data Warehouse, Customer Complaint System, EFRMS, LMS, LOS, Digital Lending Platform, Integrated Customer Care, Banking Services via WhatsApp, SMS and other Communication Channels & any other source systems which bank may mandate the vendor to integrate with DKYC & VKYC solution from time to time during the contract period.

5.13 "Dashboards" means one of the mechanisms for monitoring and measuring progress and performance of business outcome and health & performance of the systems on real time basis.

5.14 "Goods and Services" means developing, installing, configuring, customizing, integrating, implementing, supplying and maintaining of DIGITAL KYC and VIDEO KYC Solutions as per the requirement of the Bank.

6. Disclaimer

- A. The information contained in this RFP or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of CBoI, is subject to the

terms and conditions set out in this RFP.

- B. This RFP is not an offer by Central Bank of India, but an invitation to receive responses from the eligible Bidders.
- C. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This RFP does not claim to contain all the information which each Bidder may require. Each Bidder should conduct their own investigations and analysis and should check and satisfy the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advice/clarifications. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend, supplement, cancel and postpone the information in this RFP.
- D. The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.
- E. The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.
- F. The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP. Failure to furnish all information required under this RFP or to submit a Bid not substantially responsive to this RFP in all respect will be at the Bidder's risk and may result in rejection of the Bid.
- G. The issue of this RFP does not imply that the Bank is bound to select a Bidder or to award the contract to the Selected Bidder, as the case may be, for the Project and the Bank reserves the right to reject all or any of the Bids or Bidders without assigning any reason whatsoever before issuance of purchase order and/or its acceptance thereof by the successful Bidder as defined in Award Criteria and Award of Contract in this RFP.

7. Instructions to Bidders:

Bidders are expected to read, understand and follow all instructions, terms and conditions set out in the RFP. In the event of a doubt the same should be clarified from the Bank before submitting the bid.

7.1 Pre Bid Meeting

7.1.1 A pre-bid meeting will be held through physical mode (offline) or Online on the date and time mentioned in **TABLE-1**. Bidder's designated representatives (maximum two persons if attending in person) may attend the pre-bid meeting.

7.1.2 The purpose of the meeting will be to clarify the doubts raised by the probable bidders.

7.1.3 The bidders are requested to submit any queries/clarifications to the Bank on or before the date & time and the email IDs mentioned in **TABLE-1**.

7.2 Amendment of bidding document

- 7.2.1 Bank reserves the right at any time prior to the deadline for submission of bids, the Bank, for any reason, whether at its own initiative or in response to a clarification(s) requested by a prospective Bidder, may modify/ cancel/ extend/ amend the Bidding Document by modification(s) / amendment(s).
- 7.2.2 The amendments and clarification, if any, will be published on the Bank's website and GeM portal as well and will form part of the Bidding document. Signed copy of the Corrigendum/amended document and required documents: if any, should be submitted by the bidder as part of the Technical Bid.
- 7.2.3 The bid, submitted cannot be withdrawn / modified after the last date for submission of the bids unless specifically permitted in writing by the Bank.

7.3 Technical Bid

The Bidder shall furnish as part of the technical bid, necessary documents establishing the Bidder's eligibility to bid and their qualifications to perform the Contract. The documentary evidence of the Bidder's eligibility to bid and qualifications to perform the Contract if its bid is accepted, shall establish to the Bank's satisfaction that, the Bidder has the financial and technical capability necessary to perform the Contract and that, the Bidder meets the qualification requirements. Any bid document not accompanied by the above will be rejected.

Bidder shall NOT submit any information related to Commercials in the technical bid submission process or elsewhere except in Commercial Bid Submission form in e-procurement portal. Commercial bid submitted along with other documents in technical bid shall result in the disqualification of the Bid without prejudice to other rights and remedies available to the Bank as per the Terms & Conditions of the RFP

7.4 Commercial Bid

- 7.4.1 The Bank will open commercial bids of only technically qualified bidders and date and time will be intimated to technically qualified bidders, after evaluation of Technical Bid.
- 7.4.2 The calling for quote does not confer any right on the bidder for being awarded any purchase order

7.5 Bid Security (EMD)

The Bidder must fulfil following eligibility criteria:

A non-interest bearing amount as mentioned under Sl. No. 5 in **TABLE-1** should be submitted by the bidder.

7.6 Performance Bank Guarantee (PBG)

- 7.6.1 As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given in Annexure-9, for 5% of the total project cost valid for 75 months, (implementation period + 5

years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of the PO acceptance by the Bidder.

- 7.6.2 The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing bank on their letterhead. Such forwarding letter shall state that the PBG has been numbered, signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favor with authorization to sign the documents.
- 7.6.3 Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
- 7.6.4 In the event of the Successful Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.
- 7.6.5 In the event of delays by Successful Bidder in AMC support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
- 7.6.6 Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for the failure to complete their obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.
- 7.6.7 The Bank shall also be entitled to make recoveries from the Successful Bidder's bills or any other amount due, the equivalent value of any payment made to the successful bidder by the bank due to inadvertence, error, collusion, misconstruction or misstatement.
- 7.6.8 The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

8. Eligibility & Evaluation Criteria

8.1 Eligibility Criteria

SL No	Criteria	Proof of documents to be submitted
1.	Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on bid submission date.	1. Certificate of Incorporation issued by Registrar of Companies along with 2. Copies of Memorandum of Association 3. Copies of Articles of Association 4. Shareholding pattern 5. Board Resolution (As per Annexure - 31) 6. PAN, TAN, GSTIN Certificate and any other tax related document if applicable is required to be submitted along with the eligibility bid.
2.	The bidder should be an OEM (Original Equipment Manufacturer) and/or OSD (Original Solution Developer) or their authorized Service Provider in India. In case OEM/OSD participates in the tender process directly, authorized representative will not be permitted to participate in the same tender process.	Undertaking / Power of Attorney (PoA) from the OEM/ mentioning a clause that OEM/OSD will provide support services during warranty period if the bidder authorized by them fails to perform. In case of an authorized representative, a letter of authorization from original manufacturer must be furnished in original duly signed & stamped (As Annexure-6).
3.	The bidder should have a minimum annual turnover of Rs. 100 Crore per year during the last three financial years i.e. 2022-23, 2023-24 and 2024-25. This must be the individual company turnover and not of any group of companies.	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing profit, net worth and turnover of the company for the last three financial years i.e. 2022-23, 2023-24, and 2024-25 should be submitted.
4.	Bidder should have maintained an Operating Profit in at least two financial years out of the last three Financial Years i.e. 2022-23, 2023-24 and 2024-2025	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing Operating Profit.

5	The bidder should have Positive Net worth during the last three financial years i.e. 2022-23, 2023-24 and 2024-25.	Certificate from the Chartered Accountant for proceeding three years FY
6	The DKYC solution proposed by the Bidder should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and (Work Completion Certificate or Client Reference).
7	The Bidder should have <u>experience</u> in implementing the proposed DKYC solution in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and (Work Completion Certificate or Client Reference).
8	The VKYC solution <u>proposed</u> by the Bidder should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and (Work Completion Certificate or Client Reference).
9	The Bidder should have <u>experience</u> in implementing the proposed VKYC solution in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and (Work Completion Certificate or Client Reference).
10	Bidder should not have been debarred / black-listed by any Bank or RBI or any other regulatory authority or Financial Institutions in India during the currency of the RFP process (till completion of RFP process).	Letter of confirmation (self-certified letter signed by authorized official of the bidder) as per Annexure-27 should be submitted
11	The Bidder should not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity as on the date of bid submission	Self-declaration to this effect on the company's letterhead should be submitted
12	Bidder under notice/termination period from OEM/OSD as on bid submission date should not bid in this tender.	Self-declaration to this effect on the company's letterhead should be submitted.

13	The service provider should ensure that there are no legal proceedings / Inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Self-declaration to this effect on the company's letterhead should be submitted.
14	The bidder should not have: NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the bidder in the opinion of Central Bank of India to service the needs of the Bank.	Self-declaration to this effect on the company's letterhead should be submitted.
15	The Bidder is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017. or The Bidder is from such a country and has been registered with the Competent Authority i.e., the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade, as stated under Annexure to the said Office Memorandum / Order and we submit the proof of registration herewith.	Certified copy of the registration certificate as per Annexure – 13 .
16	Bidder should be certified with any one certificates among CMM Level 3 or above, ISO 27001, SOC2. (valid during the RFP process).	Supporting Document to be submitted
17	The Bidder, is not owned or controlled by any director or key officer/employee of the Bank or their relatives having the same meaning as assigned under Companies Act, 2013 and the rules framed thereunder, as amended from time to time;	Self-declaration to this effect on the company's letterhead should be submitted.

Note: -

As this shall be an additional setup parallel to the existing setup, hence the incumbent vendor is not permitted to participate in the RFP process. The bidders cannot propose the incumbent solution in response to this RFP.

In this tender process either authorized representative / distributor / dealer in India on behalf of Principal OEM/OSD (Original Equipment Manufacturer) or Principal OEM/OSD itself can bid but both cannot bid simultaneously. In such case OEM/OSD bid will only be accepted. If an agent / distributor submits bid on behalf of the Principal OEM/OSD, the same agent /

distributor shall not submit a bid on behalf of another Principal OEM/OSD in the same tender for the same item or product.

The service provider must comply with all above-mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. Documentary Evidence for compliance to each of the eligibility criteria must be enclosed along with the bid together with references. Undertaking for subsequent submission of any of the required document will not be entertained under any circumstances. However, Bank reserves the right to seek clarifications on the already submitted documents. Non-compliance of any of the criteria will entail rejection of the offer summarily. Any decision of Bank in this regard shall be final, conclusive and binding upon the service provider.

8.2 Stages of Evaluation

There would be Three (3) stages for evaluation process. The Stages are:

1. Eligibility Criteria Evaluation
2. Technical Evaluation- 70% Weightage for Technical bid
3. Commercial Evaluation- 30% Weightage for Commercial bid

A. Eligibility Criteria Evaluation:

The Eligibility would be evaluated first for the participating bidders. The bidders, who would qualify all Eligibility Criteria (Annexure-21) will be shortlisted for the technical bid evaluation.

B. Technical Evaluation

The objective of technical evaluation and shortlisting of the bidders is to facilitate the selection of the most optimal Solution(s) that appropriately meet the requirements of the Bank. The Bank will evaluate the technical offers of the bidders complying with Eligibility Criteria and the proposals meeting the said criteria will only be taken up for further technical evaluation.

As part of the technical bid, the bidder should submit all the specified documents/information covering all the clauses specified in the RFP. The eligible Bidders shall be required to deliver an exclusive presentation detailing the proposed architecture for various applications/Solutions, implementation approach, rollout strategy, etc.

The bidders should submit the soft copy of the presentation to the Bank along with their technical and commercial bids.

A bidder shall be scored based upon the scoring formula given below. Based on the scores, T1 shall be shortlisted, the decision of the Bank regarding evaluation would be final and binding on all the Bidders.

C. Evaluation of Technical Competence:

All specifications provided in this Appendix are mandatory. However, in case the mentioned feature is not immediately available, it should be customized. All customizations and integrations required shall be completed by the Bidder through respective OEMs within specified timelines without additional cost. Non-compliance with any of the specifications may render the Bidder disqualified.

Compliance with all the specifications mentioned in this Appendix must be supported by relevant and verifiable documents. All such supporting documents must be submitted along with the technical bid.

The technical bid submitted by the Bidder will be evaluated only if they fulfil the eligibility criteria. The proposal evaluation will be based on the evaluation matrix consisting of the following parameters.

Note:

The bidder should provide documentary evidence for each of the above criteria. Further the Bank's officials would visit reference sites provided by the Bidder.

Bidders scoring 70% or more marks i.e. 315 and above out of 450, will be considered eligible in technical evaluation and shall be eligible for further process of evaluation

In case there is only one bidder having technical score of 70% or more, the Bank may, at its sole discretion, also consider to reduce the threshold of 70%.

Bank may, at its sole discretion, decide to seek more information from the respondents to normalize the bids. However, respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.

Sr. No.	Criteria	Evaluation Parameter	Documentation	Normalized Max Marks
1	The <u>Proposed VKYC Solution</u> should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Count of implementations ➤ 2 - 50 Marks ➤ 1 - 30 Marks	Reference letter confirmation from the BFSI Organization that the solution is implemented & running. It should be signed (along with BFSI Organization seal) not below the Rank of CM (Scale- IV or equivalent).	50

2	The <u>Proposed DKYC Solution</u> should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Count of implementations ➤ 2 - 50 Marks ➤ 1 - 30 Marks	Reference letter confirmation from the BFSI Organization that the solution is implemented & running. It should be signed (along with BFSI Organization seal) not below the Rank of CM (Scale- IV or equivalent).	50
3	The <u>Bidder</u> should have <u>experience</u> in implementing the proposed DKYC/ VKYC solutions in at least one or more BFSI Organization in India having minimum 500 branches.	Count of implementations ➤ 2 - 50 Marks ➤ 1 - 30 Marks	Reference letter confirmation from the BFSI Organization that the solution is implemented & running. It should be signed (along with BFSI Organization seal) not below the Rank of CM (Scale- IV or equivalent).	50
4	Number of employees on the Bidders roles.	➤ Above 500 – 50 Marks ➤ Above 250 and Up to 500 – 30 Marks	Declaration supported by documentary evidence (CA Certificate)	50
5	Level of CMM Certification	➤ CMM Level 3 & Above – 25 Marks	Declaration supported by documentary evidence, should be in force at the time of bid submission	25
6	Compliance to Functional Specifications mentioned in Annexure- 29.	As per Functional Compliance based on the responses from the Bidder mentioned in RFP. The marks shall be normalized to 50.	Undertaking along with Annexure-29 should be submitted.	50

7	Compliance to Technical Specifications mentioned in Annexure- 30	As per Technical Compliance based on the responses from the Bidder mentioned in RFP. The marks shall be normalized to 50.	Undertaking along with Annexure- 30 should be submitted.	50
8	Presentation of Proposed Solution and Architecture by the Bidder/OEM & Demo of the Solution	Presentation will be evaluated on the following parameters: ➤ Quality and completeness of Proposed solution ➤ Solution architecture (scalability & flexibility) ➤ Implementation Approach & methodology ➤ Project Governance & team/ resource plan Volumes handled	Marks will be based on Presentation to technical evaluation committee.	75
9	Site Visit by DGM headed sub-committee.	Feedback from existing clients during site visit	Marks will be based on site visit by Bank's committee.	50
	Total Marks			450

D. Presentation and Demo

As part of technical evaluation process, bidder should give presentation before the evaluation committee at Mumbai. Following criteria must be adhered to by all bidders, in connection with the technical presentations during the bid selection process.

At least one senior representative from bidder's organization should be present in the technical presentations

Complete soft copies of the presentation materials should be shared with the Bank before the presentation.

The Bank will expect and demand that the key personnel showcased by the bidder in the technical presentation should be the same person that actively drives the project execution.

Bidders must strictly adhere to the time slots provided to them for the technical presentation, allowing ample time and scope for question- answers.

Focus of the presentation should be on the specifics of the solution/approach being proposed for the Bank, not on general elucidation of technologies, tool stacks or concepts.

Both technical and administrative aspects of the Assignment should be given suitable coverage.

Bidder should also present their understanding about the Bank's future requirements and approach.

Focus should be on bringing out clearly what is specific / different / novel about the approach.

All aspects of requirements in the RFP should be covered in the presentation – e.g., proposed approach, capability to develop industry grade customized products, processes, frame works, diagnostic tools, organizational capabilities, team, governance, continuous development, transition approach etc.

Any assumption, if taken in the response to RFP document should be clearly brought out in the technical presentation, along with the justification.

Bank's evaluation and scoring on all aspects including technical presentation are final and non-negotiable.

9. Commercial Evaluation

The commercial bids of only technically qualified bidders will be opened and evaluated by the Bank and the evaluation will consider the following factors:

The Bill of Material must be attached in Technical Bid as well as Commercial Bid. The format will be identical for both Technical Bid and Commercial Bid, except that the technical bid should not contain any price information (with Prices masked). Technical bid without masked Bill of Materials will be liable for rejection. Any deviations from the Bill of Material / non-submission of prices as per the format shall make the bid liable for rejection.

The optimized TCO (Total Cost of Ownership) identified in the commercial bid would be the basis of the maximum outflow of the Bank for undertaking the scope of work.

In case there is a variation between figure and words, the value mentioned in words will be considered.

In the event the vendor has not quoted / not mentioned / left blank item(s) in the commercial bid, it would be considered as free of cost. However, for the purposes of payment and finalization of the contract, the value of zero cost in the not quoted / not mentioned / left blank item(s) would be used.

Bank may waive off any minor infirmity or non-conformity or irregularity in a bid, which does not constitute a material deviation.

If there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price shall be corrected accordingly. In any case unit price cannot be increased & offered quantity cannot be decreased to correct the TCO.

If there is discrepancy between percentage and amount, the amount calculated on percentage basis will prevail.

If the bidder does not accept the correction of errors, the bid will be summarily rejected.

In all the above cases the TCO quoted as a 'Total Cost' in GeM portal would be the final price for evaluation purpose. However, TCO may be reduced to be in-line with unit price for order placement.

Discrepancies if any, would be corrected as per the TCO without increasing any of the unit price and payment would be made on unit price only.

Normalization of Bids

The Bank may go through a process of technical and/ or commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that SI/Bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that any of the bids need to be normalized and that such normalization has a bearing on the commercial bid; the Bank may at its discretion ask all the technically shortlisted SI/Bidders to resubmit the updated technical and commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission till the Bank is reasonably satisfied. The SI/Bidders agree that they have no reservation or objection to the normalization process and all the technically short listed SI/Bidders will, by responding to this detailed document, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The SI/Bidders, by submitting the response to this detailed document, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned Bidder. Bank may call for any clarifications/ additional particulars required, if any, on the technical/ commercial bids submitted. The Bidder has to submit the clarifications/ additional

particulars in writing within the specified date and time. The Bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. Bank reserves the right to call for presentation(s), product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. Central Bank of India also reserves the right to conduct reference site visits at the Bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final commercial bidding.

Note: Tendering process need not be cancelled merely on the grounds that a single tender was received provided that the single bid received is evaluated to be substantially responsive and deemed fit for award. Bank reserves right to proceed and award the tender to single bidder in case only one bidder participates in the tender / qualifies in the technical bid evaluation. Bank can negotiate with such single bidder, if required.

The Evaluation will be QCBS (Quality Cum Cost Based Solution) which is 70:30 (Technical: Commercial) i.e. The Technical Evaluation and the Commercial Evaluation shall have the weightage of 70% and 30% respectively, and this weightage shall be taken into consideration for arriving at the Successful SI/Bidder.

FINAL EVALUATION – WEIGHTED TECHNO-COMMERCIAL EVALUATION

All the bidders who qualify in the Technical evaluation process shall be considered for T score calculation. The bidders will be ranked as T1, T2 etc. based on net total score arrived basis the scoring formula mentioned below.

$$\text{Technical Score (T)} = \frac{\text{Bidder's Technical score}}{\text{Highest Technical Score}} \times 100$$

The commercial bid(s) of only those bidders, who are short-listed after technical evaluation, would be opened. The commercial score C would be calculated based on the following formula. The bidders will be ranked as C1, C2 etc. based on net total score arrived basis the scoring formula mentioned below.

$$\text{Commercial Score (C)} = \frac{\text{Lowest Commercial Price}}{\text{Bidder's Commercial Price}} \times 100$$

The final ranking of the bidders will be based on Techno Commercial evaluation i.e. 70% Weightage for Technical Score + 30% Weightage for Commercial Score. The final Score F will be calculated using the formula given below:

$$\text{Final Score (F)} = (\text{Technical Score} \times 0.7) + (\text{Commercial score} \times 0.3)$$

The bidders will be ranked as F1, F2 etc. based on net total score arrived basis the above scoring formula. The bidder who scores overall HIGHEST FINAL score F1 will be declared as winner (L1).

For example:

Three bidders namely A, B and C participated in the bid process and their technical score are as under:

$$A=60, B=80, C= 90$$

After converting them into percentile, we get

$$T \text{ for } A = (60/90) * 100 = 66.67 (T3),$$

$$T \text{ for } B = (80/90) * 100 = 88.89 (T2) \text{ and}$$

$$T \text{ for } C = (90/90) * 100 = 100 (T1)$$

The Commercial Bid prices of the bidders are as under: A= Rs.

$$8000, B= Rs. 9000, C= Rs. 10000$$

The final cost (lowest cost quoted in Commercial price bid, in this case is Rs 8000) quoted by the bidders converted into percentile score shall be as under:

$$C \text{ for } A = (8000/8000) * 100 = 100 (C1)$$

$$C \text{ for } B = (8000/9000) * 100 = 89 (C2)$$

$$C \text{ for } C = (8000/10000) * 100 = 80 (C3)$$

As the weightage for technical parameter and cost are $TW = 70\%$ and $FW = 30\%$ respectively, the final scores shall be calculated as under:

$$F \text{ for } A = (66.67*0.7) + (100*0.3) = 76.67(F3)$$

$$F \text{ for } B = (88.89*0.7) + (89*0.3) = 88.92 (F2)$$

$$F \text{ for } C = (100*0.7) + (80*0.3) = 94 (F1)$$

The proposal securing the highest combined marks and ranked F1 shall be recommended for award of contract as L1. In the event two or more bids have the same score in final ranking, the bid with highest technical score T1 will be the winner. In case of a discrepancy between amount in words and figures, the amount mentioned in words will be considered as final. Hence, the offer of bidder 'C' (being highest score) would be considered and the contract shall be awarded to 'C' at Rs. 10000, being the price quoted by C.

Note:

The bidder with highest score shall not automatically qualify for becoming selected bidder and for award of contract by the Bank. The final decision on the successful bidder will be taken by the Bank. The implementation of the project will commence upon acceptance of LOI/purchase order by the selected bidder. If for some reason, the successful bidder fails to execute an agreement within a specified timeline, the Bank reserves the right to award the contract to the next most eligible bidder based on the final evaluation scope of technical evaluation scores and commercial prices quoted during tendering process. In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder.

The Bank will calculate the scores up to two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points.

Award of Contract

The contract shall be awarded to and the order shall be placed with selected F1 Bidder (shall be called L1 bidder) securing the highest total combined score based on technical evaluation of quality and cost of the bidder. The selected bidder shall submit the acceptance of the order within seven days from the date of receipt of the order. Conditional or qualified acceptance will not be entertained and shall be rejected. On receipt of full and unconditional acceptance, bidder need to execute the required Contractual documents such as SLA, NDA, Deed of Indemnity, PBG, Escrow Agreement etc. of / with the bank in time. The effective date for start of provisional contract with the selected Bidder shall be the date of acceptance of the order by the bidder. Bank reserves its right to consider at its sole discretion the late acceptance of the order by selected bidder (s).

10. SCOPE OF WORK

A. Functional Scope of Work:

1. General Scope

1.1 Objective

To implement a secure, compliant, AI-powered, scalable, and omni-channel Video-CIP/Digital KYC platform that enables seamless end-to-end digital customer on-boarding. The platform shall comply with:

- RBI Master KYC Directions
- Digital Personal Data Protection (DPDP) Act
- Relevant data protection and financial sector regulations
- Banks Policy or any other regulator
- CKYC
- V-CIP guidelines

- Integration with Mule Hunter for detecting fraud
- Any other Regulatory guidelines from time to time

1.2 Customer Segments Covered

1.2.1 New-to-Bank (NTB) Customer Onboarding

a. Retail Customers (Personal Accounts)

- Minor, General, Salary, NRE, NRO, Student, Pensioner, Differently Abled (Divyang), Custom Schemes, Credit Card
- Current Account – Individual
- Term Deposit / Recurring Deposit
- PMJDY

b. Corporate Customers /Non-Personal Accounts

- Sole Proprietorships
- Partnerships
- Limited Liability Partnerships (LLPs)
- Public/Private Limited Companies
- Societies and Trusts/NGOs/Clubs
- Government and Quasi-Government Entities
- SHG

c. Social Security Schemes

- Public Provident Fund (PPF)
- Sukanya Samriddhi Yojana (SSY)
- Senior Citizen Savings Scheme (SCSS) or
- Any other Government Sponsored schemes

1.2.2 Services for Existing-to-Bank (ETB) Customers

The solution must also support the following services for existing customers:

- Digital Re-KYC through Video KYC
- CIF or account generation (Personal, Non-Personal& Social security schemes)
- Pension Life Certificate submission/update
- Conversion of inoperative accounts to operative
- Integration with product journeys such as Digital Lending Platform:
 - Personal Loans (PL)
 - Home Loans (HL)
 - Mortgage Loans (ML)
 - CKCC or other accounts
 - Insurance
 - Composite Account Opening and Cross-Selling within the journey
 - Credit Card
 - Mutual Fund Investments

2. Scope of Video KYC through VCIP

2.1 Customer/User On-boarding Journey

The solution must support a seamless on-boarding journey accessible via Web and Mobile Customer Portals, with features enabling customer engagement through:

- Journey link (URL) delivery via:
 - WhatsApp
 - SMS/Email
 - Internet/Mobile Banking apps
 - Social Media Platforms or Any additional digital channels
- Journey Link Requirements:
 - Unique and time-bound links
 - Linked to specific application/reference ID
 - Support for retry or re-initiation within the validity window
 - UTM tracking capabilities for campaign and source attribution

2.2 Customer Interface Specifications

- Location-Based Branch Auto-Selection
- Automatically suggest the nearest bank branch based on the customer's geo-location.
- Pre-fill branch name and code in the application form, editable by the customer.
- Officially Valid Document (OVD) Upload & Auto-Population
- Support for uploading OVDs in PDF, JPG, or PNG format via:
 - Local device
 - DigiLocker integration
 - Live capture using device camera
 - CKYCR integration in with option to search and download in any format.
- Supported OVDs:
 - Aadhaar (XML/QR)
 - PAN
 - Passport
 - Voter ID
 - Driving License
 - Any other OVDs prescribed by Regulator
- For non-personal customers:
 - Udyam Aadhaar,
 - GST,
 - Shop Establishment Certificate,
 - Import/Export Certificates,
 - Partnership Deeds,
 - Agreements,
 - MoA,
 - AoA, etc.
- Key Capabilities:
 - OCR-based data extraction
 - Checksum validation

- Auto-fill: Name, DOB, Gender, Address, Document Number, Issuing Authority
- Manual confirmation prompt for users
- Document classification and recognition
- Geotagged watermark with timestamp on uploaded OVDs/images and or any other documents
- Customer's Email validation through OTP
- Application Download & Email Sharing Upon form submission:
 - Allow users to download the filled application as a PDF
 - Option to email the PDF to the registered or alternate email ID
- Session Resume and Status Tracking
Ability for customers to:
 - Resume missed/dropped sessions
 - Track statuses: In Progress, Scheduled, Under Review, Approved, Rejected
 - Receive automated real-time updates via WhatsApp, SMS, and Email
- Cross-Device & Multi-Lingual Support
 - Optimized UI for desktops, tablets, and mobile devices
 - Interface in multiple Indian languages minimum 12
 - Auto-language detection based on browser/app settings
 - Manual language switcher on all screens
- Accessibility & UX Design
 - Compliance with WCAG 3.0 standards:
 - Keyboard navigation
 - Screen-reader compatibility
 - Adjustable font size and color contrast
 - Step-by-step flow with progress indicators and contextual tooltips

2.3 Integration with Bank Systems

- The platform must integrate with the following systems and solutions directly or through Bank's Middleware:
 - Omni-channel platforms
 - Lead Management System (LMS)
 - Digital Lending Platform (DLP)
 - Supply Chain Finance Platform(SCF)
 - MarTech (Marketing Automation) Platform / CRM
 - Integrated Customer Care (ICC)
 - Core Banking Solution (CBS)
 - Active Directory (AD) and HRMS etc.
 - Integration with any other system

2.4 Video-CIP Session Management

a) Secure Video Interaction Capabilities

The solution must support:

- Browser-based or in-app live video interaction between customer and agent
- Assistance via Co Browsing, Chatbot,
- Two-way audio-video capture with:
 - Liveliness detection
 - Face match against submitted photo IDs
 - Geo-tagging and DigiPIN capture for location validation
- OCR-based auto-fill from uploaded or live-captured documents
 - Document fetch via DigiLocker, local storage, or camera
- Session security with encryption and compliance with audit logging

b) Session Scheduling, Rescheduling, and Notifications Customer-Driven Time Slot Booking

- Customers should be able to schedule or reschedule Video-CIP sessions through:
- Web or mobile portal
- Assisted channels (branch, call center, agent-assisted app)

C) Core Features

- Multilingual interface with regional time-zone support
- Smart scheduling based on:
 - Agent availability
 - Preferred language
 - Customer category (e.g., Senior Citizen, NRI, Priority, Divyang)
- Real-time slot availability calendar (agent-wise)
- Configurable session duration (e.g., 15-minute intervals)
- Rescheduling and cancellation options within permissible windows, per RBI/bank policy
- Auto-detection of time zone and language
- Retry links sent via SMS, Email, WhatsApp

2.5 Advanced Agent Assignment & Call Routing

a) Multilingual agent assignment based on:

- Customer-selected language
- Agent location and availability
- Ad-hoc/manual override for special handling

b) Distribution logic:

- AI or rules-based auto-routing for fair distribution and load balancing
- Option for manual assignment where needed
- Auto re-routing:
 - Reconnects to the same agent within a defined time in case of call drop
 - Automatic reassignment if selected agent/language is unavailable

c) Session notifications over:

- IVR

- SMS/Email
 - WhatsApp
 - Integrated Customer Care Center (ICC) or Bot interaction
- d) Triggers to ICC for manual outreach when required
- e) Queue Management and Prioritization
- f) Dynamic Queue Handling
- g) Maintain VCIP queues segmented by:
- h) Customer type (Retail, Corporate, NRI)
- i) Session status (Scheduled, Missed, Retry, In Progress)
- j) Channel (Online, Agent-assisted)
- k) Intelligent load distribution across:
- l) Languages
- m) Time zones
- n) Agent availability
- o) Queue priority management:
- p) Auto or manual prioritization for:
- q) Senior citizens
- r) Differently abled (Divyang)
- s) Minors
- t) High-value or priority customers
- u) AI-based rescheduling when a customer's preferred agent is not available

2.6 Missed Session & Retry Handling

- a) Auto-detection of:
- No-show by agent or customer
 - Technical disruptions (network/device failure)
 - Early termination or incomplete sessions
- b) Retry mechanisms:
- Send new link to retry immediately or reschedule
 - Notify back office for manual intervention if multiple retries fail
 - Ensure single video file per session, even in case of reconnection

c) Call Distribution and Escalation Handling

- Agent segmentation based on:
 - Geography
 - Language
 - Risk/customer profile
 - Escalation for flagged sessions (e.g., fuzzy face match, document mismatch)
- Support agent-to-agent handover in case of routing failure or drop
- Full session traceability via integrated audit module

2.7 AI & Fraud Detection

The solution must provide built-in AI capabilities to detect and prevent identity fraud. Features should include:

a) Passive & Real-Time Checks

- Liveliness detection without active prompts
- Face match scoring with bank-configurable thresholds
- Detection of:
 - Deep-fakes
 - Spoof attempts
 - Virtual cameras
 - Screen sharing or remote access tools
 - Multiple faces in frame
- Unusual voice tone or background noise

b) Document Integrity Verification

- Tamper detection in uploaded OVDs
- Anomaly detection in images (e.g., blur, glare, manipulation)
- Fraud alert triggers based on:
 - Geo location
 - PIN code/DigiPIN
 - Document or customer behavior anomalies
 - Links to banned entities (e.g., NGOs flagged by bank/RBI)
 - Maintain Negative Registry and have a Check mechanism

2.8 Data Capture and Customer Interface

a) Interactive & Responsive Webpages

- Optimized for desktop, mobile, and tablet
- Compatible with all major browsers
- Multilingual web interface with configurable fields

b) Data Accuracy Features

- Minimize manual entry-
- Auto-population from OVDs
- Dropdowns and controlled lists for key inputs

c) Assistance options via:

- Audio call
- Chat
- Video call
- Co-browsing
- Auto-save progress during drop-offs and session resumes

d) Secure Data Management

- All data to be stored in encrypted form on the bank's domain
- Consent management aligned with:
 - DPDP Act
 - RBI guidelines

- Any other applicable data protection laws
- Support for both mandatory and optional consents
- Store geo-coordinates and DigiPIN at capture points

2.9 Marketing & Consent-Driven Outreach

Capture source of traffic via:

- Social media
- Paid digital campaigns
- Search engine marketing
- Validate contact details and social handles (Email, Instagram, Facebook)
- Consent-driven data capture with purpose limitation and opt-out options
- Lead tagging to MarTech platform for campaign attribution

2.10 Identity Validation Capabilities

a) Aadhaar Validation

- Via OTP, biometric, facial recognition, or iris
- Support Aadhaar XML not older than 3 working days, as per RBI norms

b) PAN Validation

- Validate via NSDL integration

c) Other OVD Validation

- Via DigiLocker or third-party APIs (e.g., Protean, UIDAI)
- CKYC integration for data fetch and upload to CERSAI.
- Demographic Details
 - Auto-fetch:
 - Name
 - Address
 - Photo from OVDs

d) Liveliness & Face Match

- Ensure face match with photo IDs using facial recognition
- Detect presence (anti-spoofing measures)
- Identify presence of multiple faces in the frame
- Perform well even under:
 - Lighting variations
 - Weight changes
 - Ageing

e) De-duplication

- Cross-check new customer details (Mobile, Aadhaar, PAN, etc.) against CBS
- Configurable rules to auto-pass or flag suspect duplicates

2.11 Agent & Auditor Interfaces

a) Agent Interaction Portal

The Agent Portal must facilitate efficient and compliant customer interactions, ensuring adherence to KYC guidelines. Key features include:

- Pre-Interaction Capabilities
- Preview and review:
 - Customer-submitted OVDs
 - Pre-filled application details
- Device and accessory support:
 - Desktop, Tablet, Mobile
 - Headphone, mic, touch input
- Manual and automated call handling:
 - Accept/reject calls with mandatory reason logging
- Auto-routing based on:
 - Agent availability
 - Language proficiency
 - Geography

b) During Video Session

- Live two-way interaction (audio/video/chat)
- Document and screen sharing
- Liveliness check via facial expressions/blinking (no pre-recorded video allowed)
- Random question prompts for identity confirmation
- Face matching between selfie and OVD photos
- Name and face match scoring visible with defined thresholds
- Geo-location tagging via GPS/NAVIC
- Auto-reconnect if session disconnects

c) Agent Controls & Features

- Volume control, mute/unmute, replay on demand
- Capture photo via front/back camera
- Document editing (if permitted)
- Mark mobile numbers or customers as suspicious (with remarks)
 - Enable additional features or cross-sell products during call
- Trigger fraud alerts based on:
 - Mobile number
 - Location
 - PIN code/DigiPIN
 - Linked NGO or banned entities
- Lead and offer integration with MarTech platform
- Raise ICC alerts if customer is unreachable or non-responsive

d) Auditor Portal

The Auditor Portal enables post-interaction review, validation, and final approval. Key features include:

- Interaction Review
 - Access all session recordings (live or low-bandwidth compressed stream)
 - Review all submitted documents:
 - Zoom in/out
 - Download
 - Highlight key fields
- Verification Controls
- Decision options:
 - Approve
 - Reject (with reason)
 - Request correction or clarification (Push Back to Agent)
 - View and manage schedule:
 - By language, date, time, customer type, location
 - Translate audio/video as needed for clarity
- Dashboards for:
 - Pending
 - Completed
 - Rejected interactions
 - Status at CBS level

e) Additional Capabilities

- Raise fraud alerts based on captured data or location behavior
- Mark sessions or customers as high-risk/suspicious
- Upgrade products or facilities based on interaction findings
- Escalate back to agents with comments
- Final authorization of account opening — no account should be opened without auditor's approval

2.12 Post-Audit Auto Triggers

Upon approval, the following must be auto triggered:

- CIF creation
- Account opening (all variants)
- Issuance of:
 - Debit Card/ Passbook/ Cheque Book
 - Mobile/Internet Banking
 - Sound Box or other digital tools

2.13 Account Funding Triggers

- API/Link to be auto sent to customer for funding newly opened account
- Integration with notification engines (SMS, Email, WhatsApp, IVR, ICC)
- Monitor account status post-onboarding and send reminders for account funding

2.14 Verification Portal & Field Verification

a) Central Verification Portal

Schedule and monitor physical or virtual verification of:

- ID
- Address
- Business or Establishment details
- Capture:
 - Photographs of location/premises
 - Geo-coordinates (PIN and DigiPIN)
 - MIS Dashboard to monitor:
 - Verified vs. non-verified accounts
 - Verification turnaround time
 - Exception or escalation cases

b) Verification Agency Integration

API readiness to integrate with:

- In-house verification teams
- External verification agencies
- Track activities and performance of verification agencies
- Maintain audit logs and status history for each account

2.15 Payment Options

The solution must support seamless integration with multiple Payment Aggregators to allow customers to fund their accounts post-creation. Customer should be redirected to payment page securely via:

- UPI
- Net Banking
- Debit Card
- Other supported digital modes
- Payment status should be updated in real time and stored in onboarding records
- APIs must handle:
 - Payment confirmation
 - Failure handling and retry options

2.16 Exception Handling

The platform should have robust mechanisms to handle:

- Aborted sessions due to technical failure, customer drop-offs, or system errors
- Auto-retry or manual handling workflows for:
 - Incomplete KYC
 - Failed API calls
 - Payment issues
 - Verification issues
- Exception handling should:
 - Be auditable
 - Allow rule-based escalation
 - Maintain complete logs

2.17 AI Capabilities

The solution must include advanced AI-driven features for security, compliance, and personalization:

a) KYC Validation

- Face match scoring with thresholds defined by bank/RBI
- Passive and active liveness detection
- Detect spoofing and presentation attacks

b) Behavioral Intelligence

- Alert agents for unusual activity patterns, such as:
 - Suspicious browser plug-ins
 - Unusual document formats
 - Rapid-clicking or evasion patterns
- AI-based flagging for:
 - Deepfakes
 - Tampered documents
 - Multi-face detection

c) Customer Segmentation

- AI engine to classify customer profile (e.g., HNI, SME, Retail)
- Recommend product prompts based on:
- Income/employment info
- Geolocation
- Existing bank relationships

2.18 Third-Party Integrations

a) Solution must support API-based integration with:

- UIDAI (Aadhaar validation)
- NSDL (PAN validation)
- DigiLocker
- Protean/Other OVD Verifiers
- CMS (ATM switch)
- CDSL
- CBS
- DLP (Digital Lending)
- ICC (Integrated Contact Center)
- MarTech/CRM
- E-sign and E-mandate platforms
- Payment Gateways
- Account Aggregator (AA) ecosystem

b) All integrations should:

- Be modular and easily configurable
- Be secured with encryption and tokenization
- Log audit trails for each invocation

2.19 MIS Reports & Analytics

a) The platform must provide customizable MIS reports for:

- Customer journey stage (Scheduled, In-progress, Completed, Failed)
- Customers Captured data like Customer ID, Photo, Video etc.

b) Agent and auditor performance

- API success/failure rates
- Re-KYC vs. NTB breakdowns
- Region/zone/branch performance
- Product conversion ratios (cross-sell leads, actual conversion)
- Funding status and payment channel analytics

c) Reports must be:

- Downloadable in multiple formats (TEXT, CSV, Excel, PDF etc.)
- Schedule-ready and filterable
- Accessible by authorized users based on roles
- Branch/RO/ZO/CO portal
- Customized Dashboard for Branches to monitor their accounts
- Customized Dashboard for Regional Offices (RO) to monitor their branches
- Customized Dashboard for Zonal Offices to monitor their ROs and Branches
- Customized Dashboard for Central Office to monitor ZO, RO and Branches
- Search, view and download the documents shared by customers and generated by the portal

2.20 Information & Cyber Security Requirements

a) All information security practices must comply with:

- RBI's Cyber Security Framework for Banks and or any other regulatory bodies
- DPDP Act
- Bank's internal information security policies

b) Security Standards

- End-to-end encryption (data at rest and in transit)
- Secure session handling and role-based access control
- Secure APIs with authentication and throttling
- On-premises or VPC-hosted as per bank's architecture

c) Integration with:

- Bank's SIEM/Log Management tools
- Vulnerability and patch management solutions

d) Channel Communications

- Secure multi-lingual notifications across:
 - SMS/Email
 - WhatsApp
 - In-App/Browser push
 - ICC and bot-assisted calls

2.21 Network Health & Performance Monitoring

- Real-time health checks before session initiation
- Bandwidth checks at both customer and agent ends
- Display of network strength during session
- Support for low-bandwidth optimization for rural/semi-urban users without compromising the quality
- Single Sign-On (SSO) & Role-Based Access
- Unified agent login for all journeys (e.g., SB, PL, HL)
- Distinct identifiers for each business journey for audit/logging

3. For Digital KYC (DKYC) Platform – Advanced Scope

3.1 Objective

This project enables bank staff-assisted Digital KYC onboarding through tablet devices or any OS compatible digital device. The application ensures seamless data capture, document validation, and biometric checks with minimal manual input. It provides a secure, audited, and role-based interface for Makers, Checkers, Admins, and Auditors.

- The platform must eliminate manual account opening and support maker-checker-based validation, liveness and fraud detection, campaign execution, and seamless integration with core banking, HRMS, and external verification systems. To deploy a robust DKYC solution that Digitizes all customer onboarding processes across branches, BC outlets, and digital channels.
- Ensures compliance with RBI KYC Master Direction and latest circular and or any regulatory bodies directions.
- Supports AI-based liveness detection, face match, and fraud detection.
- Incorporates maker-checker workflows, low-bandwidth optimization, and marketing-led campaign initiation.
- Seamlessly integrates with HRMS, Active Directory, CBS, CKYC, and Aadhaar/PAN APIs.

3.2 Functional Scope

a) Onboarding Journey Features

- User Interface & Scalability
 - Fast, lightweight interface optimized for low-bandwidth users
 - Mobile, tablet, desktop responsive UI
 - Multilingual interface (Indian languages)
 - Admin panel for easy variant creation/modification

- Scalable to support over 50,000 DKYC sessions/day without any limit

3.3 Key Functional Components

a) Platform Compatibility

- Application must be OS-agnostic – compatible with Android, iOS, and Web platforms.
- Should be optimized for tablets, mobile devices, and laptops/desktops.

b) User Roles

- Maker (Bank staff who initiates KYC)
- Checker (Bank official who verifies KYC and approves/rejects)
- Auditor (Read-only access for compliance audit)
- Admin (Manages user access, roles, session logs, etc.)

c) Authentication & User Access Control

- Auto-block DKYC platform access for: Employees marked as on leave, retired, or inactive in HRMS
- Role-based access for:
 - Makers,
 - Checkers,
 - Branch Admins,
 - Super Admins,
 - Marketing Users
- Session logging with role, timestamp, and device info
- Auto assessing Role for maker and checker based on HRMS API response
- Branch selection:
 - Auto branch selection for branch employees
 - Optional selection for Marketing staffs

d) Maker-Checker Workflow

- Maker uploads documents, fills forms, and submits session
- Checker reviews, approves, or pushes back with comments
- Push-back visible to maker with rework ability
- Status History: Draft, Submitted, Pushed Back, Approved, Rejected
- Audit logs for all actions by Maker and Checker
- Notifications for both roles on action/status updates

3.4 Maker Controls & Features

a) Maker-Level Workflow

- Authentication -
Dual-layer authentication for Makers:
 - Active Directory (AD) login
 - HRMS validation (active status – not on leave, retired, or resigned)
 - OTP-based authentication on registered mobile/email

b) KYC Capture Process

- Digital KYC form with:
 - Minimal manual entry: Majority of fields auto-filled using backend integrations
 - Dynamic forms based on OVD selected
 - Customer's Email validation through OTP
- OVD validation via APIs (Aadhaar, PAN, Driving License, Passport/Non personal Proofs)
- Capture of:
 - Photograph using in-device camera
 - Live Selfie (must pass liveness detection)
 - Real-time validation and prompt for retake
- Document upload (real-time image capture, PDF/photo)
- Face match between OVD photo and selfie (via AI/ML)
- Liveness Check:
 - Block blurred, tilted, photocopied, or poor-quality images
- Consent Capture:
 - Checkbox + OTP verification
- Digital consent stored as part of audit trail
 - Enable additional features or cross-sell products during the session
 - Geo-location tagging via GPS/NAVIC

c) Checker-Level Workflow

The Auditor Portal enables post-interaction review, validation, and final approval of session submitted by maker. Key features include:

- Interaction Review
 - Access all session details
 - Review all submitted documents:
 - Download
- Verification Controls
- Decision options:
 - Approve
 - Reject (with reason)
 - Push back to Maker for rework (reopens edit access)
- Full visibility of:
 - Captured data
 - Documents
 - Face match result
 - Liveness score
- Application routing based on role and region/branch mapping
- Trigger fraud alerts based on:
 - Mobile number: Mark mobile numbers or customers as suspicious (with remarks)
 - Location
 - PIN code/DigiPIN
 - Linked NGO or banned entities

d) Reporting & Admin Portals

Role-based access configuration

- Branch-Level Admin Portal
 - View DKYC sessions for respective branch
 - Maker-Checker dashboards with filters
 - Downloadable MIS reports (PDF, Excel)
 - Session tracking and monitoring
- Super Admin Portal
 - Cross-branch monitoring
 - Create/edit/delete variants, workflows, users
 - System-wide audit logs and compliance reports
 - Export reports by: Date, product type, region, status, user
- Integration dashboard for OVD API status
- Notification manager (SMS/Email templates for consent, welcome msg, rejection reasons, etc.)

e) Audit Trail

- Every action (create, update, submit, approve, reject) should be logged with:
- Timestamp
- User ID and role
- IP and device metadata
- Dedicated Auditor role with read-only access to completed applications and full audit logs

3.5 Security & Compliance

- End-to-End Encryption of all data in transit and at rest
- Integration with HRMS for active employee check
- Session Timeout & auto-logout after inactivity
- IP whitelisting for internal users (optional)
- Data masking for sensitive fields (PAN, Aadhaar)
- Compliance with RBI KYC Master Directions, UIDAI norms, and IT Act 2000

3.6 Scalability & Performance

- Auto-scaling support for API and application layer
- Session retrieval and auto-resume in case of network/API failure
- Offline mode with encrypted local cache and sync on reconnect

3.7 Notifications & Communication

- Real-time SMS/Email alerts to customers:
 - Welcome Message
 - Application submission confirmation
 - Consent capture
 - Rejection or approval intimation
 - Configurable templates at the branch level or admin panel

3.8 Reports & Analytics

- Realtime Dashboards for:
 - Applications initiated, submitted, approved, rejected
- TAT analysis per Maker/Checker/Branch
- API response logs and error trends
- Exportable reports in PDF/Excel format

3.9 Additional Capabilities

- Raise fraud alerts based on captured data or location behavior
- Mark sessions or customers as high-risk/suspicious
- Upgrade products or facilities based on interaction findings
- Escalate back to agents with comments
- Final authorization of account opening — no account should be opened without checker's approval

3.10 Post-Audit Auto Triggers

- Upon approval, the following must be auto triggered:
- CIF creation
- Account opening (all variants)
- Issuance of:
 - Debit Card/ Passbook/ Cheque Book
 - Mobile/Internet Banking
 - Sound Box or other digital tools

3.11 Campaign Mode & Marketing Team Access

- Dedicated interface for marketing/acquisition teams
- Launch bulk DKYC journeys through campaign mode
- Track source-wise journey initiation, completion, and conversion

3.12 Notification Engine

Real-time alerts via SMS, Email, WhatsApp

- Welcome message on journey start
- Consent acknowledgement
- Account/KYC status updates
- Session resumption/reminder prompts

3.13 Accessibility & UX Design

- Compliance with WCAG 3.0 standards:
- Keyboard navigation
- Screen-reader compatibility
- Adjustable font size and color contrast
- Step-by-step flow with progress indicators and contextual tooltips

3.14 Integration with Bank Systems

The platform must integrate with the following systems and solutions:

- Omni-channel platforms
- Lead Management System (LMS)
- Digital Lending Platform (DLP)
- Supply Chain Finance Platform
- MarTech (Marketing Automation) Platform
- Integrated Customer Care (ICC)
- Core Banking Solution (CBS)
- Active Directory (AD) and HRMS etc.

3.15 Retry mechanisms:

- Auto retrigger without to retry immediately or reschedule

3.16 AI & Fraud Detection

The solution must provide built-in AI capabilities to detect and prevent identity fraud.

Features should include:

a) Passive & Real-Time Checks

- Liveness detection without active prompts
- Face match scoring with bank-configurable thresholds
- Detection of:
 - Multiple faces in frame
 - Brightness check
 - Auto retake for blurred or tilted image

b) Document Integrity Verification

- Tamper detection in uploaded OVDs
- Anomaly detection in images (e.g., blur, glare, manipulation)
- Fraud alert triggers based on:
 - Geo location
 - PIN code/DigiPIN
 - Document or customer behavior anomalies
 - Links to banned entities (e.g., NGOs flagged by bank/RBI)

c) Data Capture and Customer Interface

- Interactive & Responsive Webpages
 - Optimized for desktop, mobile, and tablet
 - Compatible with all major browsers
 - Multilingual web interface with configurable fields
- Data Accuracy Features
 - Minimize manual entry-
 - Auto-population from OVDs
 - Dropdowns and controlled lists for key inputs
 - Auto-save progress during drop-offs and session resumes

3.17 Secure Data Management

- All data to be stored in encrypted form on the bank's domain
- Consent management aligned with:
 - DPDP Act
 - RBI guidelines
 - Any other applicable data protection laws
- Support for both mandatory and optional consents
- Store geo-coordinates and DigiPIN at capture points

3.18 Identity Validation Capabilities

- Aadhaar Validation
 - Via OTP, biometric, facial recognition, or iris
 - Support only Aadhaar XML not older than 3 working days, as per RBI norms
- PAN Validation
 - Validate via NSDL integration
- Other OVD Validation
 - Via DigiLocker or third-party APIs (e.g., Protean, UIDAI)
 - CKYC integration for data fetch, download and upload to CERSAI.
 - Demographic Details
- Auto-fetch:
 - Name
 - Address
 - Photo from OVDs
 - De-duplication
 - Cross-check new customer details (Mobile, Aadhaar, PAN, etc.) against CBS
 - Configurable rules to auto-pass or flag suspect duplicates
 - Account Funding Triggers
 - API/Link to be auto sent to customer for funding newly opened account
 - Integration with notification engines (SMS, Email, WhatsApp, IVR, ICC)
 - Monitor account status post-onboarding and send reminders for account funding

3.19 Verification Portal & Field Verification

a) Central Verification Portal

- Schedule and monitor physical or virtual verification of:
 - ID
 - Address
 - Business or Establishment details
 - Capture:
 - Photographs of location/premises
 - Geo-coordinates (PIN and DigiPIN)
 - MIS Dashboard to monitor:
 - Verified vs. non-verified accounts
 - Verification turnaround time
 - Exception or escalation cases

b) Verification Agency Integration

- API readiness to integrate with:
 - In-house verification teams
 - External verification agencies
 - Track activities and performance of verification agencies
 - Maintain audit logs and status history for each account

3.20 Exception Handling

a) The platform should have robust mechanisms to handle:

- Aborted sessions due to technical failure, customer drop-offs, or system errors
- Auto-retry for:
 - Incomplete KYC
 - Failed API calls
 - Payment issues
 - Verification issues

b) Exception handling should:

- Be auditable
- Allow rule-based escalation
- Maintain complete logs

3.21 AI Capabilities

The solution must include advanced AI-driven features for security, compliance, and personalization:

a) KYC Validation

- Face match scoring with thresholds defined by bank/RBI
- Passive and active liveliness detection
- Detect spoofing and presentation attacks

b) Behavioral Intelligence

- Alert agents for unusual activity patterns, such as:
 - Unusual document formats
- AI-based flagging for:
 - Deepfakes
 - Tampered documents
 - Multi-face detection

c) Customer Segmentation

- AI engine to classify customer profile (e.g. HNI, SME, Retail)
- Recommend product prompts based on:
 - Income/employment info
 - Geolocation
 - Existing bank relationships

3.22 Third-Party Integrations

- Solution must support API-based integration with:

- UIDAI (Aadhaar validation)
- NSDL (PAN validation)
- DigiLocker
- Protean/Other OVD Verifiers
- CMS (ATM switch)
- CDSL
- CBS
- DLP (Digital Lending)
- ICC (Integrated Contact Center)
- MarTech/CRM
- E-sign and E-mandate platforms
- Payment Gateways
- Account Aggregator (AA) ecosystem
- All integrations should:
- Be modular and easily configurable
- Be secured with encryption and tokenization
- Log audit trails for each invocation

3.33 MIS Reports

a) The platform must provide customizable MIS reports for:

- Customer journey stage (Scheduled, In-progress, Completed, Failed)
- Agent and auditor performance
- API success/failure rates
- Region/zone/branch performance
- Product conversion ratios (cross-sell leads, actual conversion)
- Funding status and payment channel analytics

b) Reports must be:

- Downloadable in multiple formats (CSV, Excel, PDF)
- Schedule-ready and filterable
- Accessible by authorized users based on roles

3.34 Information & Cyber Security Requirements

a) All information security practices must comply with:

- RBI's Cyber Security Framework for Banks
- DPDP Act
- Bank's internal information security policies
- b) Security Standards
- End-to-end encryption (data at rest and in transit)
- Secure session handling and role-based access control
- Secure APIs with authentication and throttling
- On-premises or VPC-hosted as per bank's architecture

b) Integration with:

- Bank's SIEM/Log Management tools
- Vulnerability and patch management solutions

c) Channel Communications

- Secure multi-lingual notifications across:
 - SMS/Email
 - WhatsApp
 - In-App/Browser push
 - ICC and bot-assisted calls

3.35 Network Health & Performance Monitoring

- Real-time health checks before session initiation
- Bandwidth checks at both customer and agent ends
- Display of network strength during session
- Support for low-bandwidth optimization for rural/semi-urban users
- Single Sign-On (SSO) & Role-Based Access
- Distinct identifiers for each business journey for audit/logging
- API communication secured via tokenization and mutual authentication
- Audit log encryption and tamper detection

3.36 Compliance with:

- RBI Cyber Security Framework and or other regulatory body compliance
- DPDP Act, 2023
- Bank's internal security policies

3.37 Additional Features

- Support for Campaign-based KYC drives by Marketing Team (separate role access)
- Dynamic form flow for different account types or customer segments

3.38 Customer-Initiated DKYC and Maker-Checker Workflow

- a) Customer Self-Initiated DKYC Form Submission
- The solution shall enable an option for customers to initiate and fill the Digital KYC (DKYC) form themselves through a secure digital interface (mobile or web). This self-fill functionality should support:
 - Secure login and OTP-based authentication.
 - Data pre-fill (wherever applicable) to enhance user convenience.
 - Real-time data validation and form completeness checks.
 - Submission of completed application forms to the bank's DKYC platform for further processing.

b) Maker-Assisted Verification and Authentication

- All self-submitted DKYC applications shall be routed to a designated Maker (Bank Staff/Agent) for assisted verification. The Maker shall perform the following tasks:
 - Capture of live image/selfie of the customer.
 - Capture of Officially Valid Documents (OVDs) such as Aadhaar, PAN, Passport, etc.

- Perform facial matching between the live selfie and the photo on the submitted ID proof.
- Conduct liveness detection to prevent fraud and ensure real presence of the customer.
- Add timestamp and maker credentials to the session and submit the application to the Checker.

c) Checker-Level Verification and Approval

- The verified application shall be forwarded to the Checker for review and final approval. The Checker should have access to:
 - Customer details submitted via self-fill and verified by the Maker.
 - Captured selfie, ID proof images, and system-generated facial match and liveness results.
 - Audit logs with timestamps and user details for all maker-level actions.

d) Bulk Upload Capability for Organizational Accounts

- The platform must support bulk form upload functionality for onboarding organizational/non-individual accounts. The system should:
 - Allow upload of multiple DKYC forms in prescribed format (e.g., Excel, CSV, or JSON).
 - Create individual sessions for each account under the bulk upload.
 - Enable the Maker to access each session separately for document capture, selfie validation, and authentication.
 - Route each session to the Checker for review and approval as per standard workflow.

4. Pension Life Certificate (PLC) Updation through VKYC or Branch-assisted Digital KYC for Existing Bank Pensioners

4.1. Objective

To enable the Bank's existing pensioners, including retired staff and pension account holders, to submit their annual life certificate digitally, either via Video KYC (VKYC) or through branch-assisted Digital KYC, ensuring convenience, compliance, and operational efficiency.

4.2 High-Level Process Flow

a) Initiation of Digital Form:

- Pensioner accesses a digital application form via mobile, tablet, or web interface and submit the application for VKYC approval .or can choose DKYC through branch assisted mode for submission of PLC.
- System performs deduplication (De-dupe) checks using customer identifiers (e.g., CIF, PAN, Aadhaar, mobile number).
- Confirms the applicant is an existing customer of the Bank.

b) Pensioner Type Selection:

- Applicant selects their pensioner category (e.g., Bank Retired Staff, Government Pensioner, Other Pension Account Holders).
- c) Aadhaar Authentication:
 - Performed via UIDAI APIs (eKYC, Aadhaar XML, OTP, or biometric).
 - Customer consent must be captured digitally.
- d) Choice of Verification Mode:
 - After form submission and Aadhaar authentication, the pensioner may choose one of two KYC verification modes:
 - Video KYC (VKYC) – Remote Self-Service
 - Digital KYC (DKYC) – Branch Official Assisted via Tablet/Device
- e) Functional Requirements: To follow applicable requirements as per VCIP or DKYC
 - Upon approval (via VKYC or DKYC):
 - Life certificate status is automatically updated in:
 - Pension Management System
 - HRMS (for retired staff)
 - CBS (if linked to pension account)
 - Notification to be sent to customer via SMS/Email confirming submission.
- f) Integrations Required
 - CBS for customer verification and life certificate update
 - HRMS for retired staff validation
 - UIDAI Aadhaar Authentication APIs
 - Notification APIs (SMS, Email)
 - Branch admin panel and central admin dashboard

5. ReKYC through VKYC or Branch-assisted Digital KYC for Existing Bank customers

5.1 Objective

To enable digital ReKYC for existing customers (both personal and non-personal) who are due for KYC revalidation or whose accounts are inoperative, using dedupe APIs for identification, Aadhaar and PAN validation, and VKYC for updated KYC/address information.

5.2 Customer Categories Covered

- Personal Customers: Individuals with Savings, Current, or Term Deposit accounts
- Non-Personal Customers: Entities such as firms, trusts, HUFs, companies (where allowed via digital process)
- Status Covered:
 - Customers due for periodic ReKYC
 - Updating of customer data
 - Inoperative and or DEAF account holders (as per RBI guidelines)

5.3 High-Level Process Flow

a) Initiation:

- Customer accesses the ReKYC portal (web/mobile/tablet interface).
- Enters registered mobile number for identification.

b) Customer Identification via De-dupe API:

- System fetches customer details, Inoperative or DEAF status using registered mobile number and validates using backend de-dupe APIs (using mobile, PAN, Aadhaar).

c) Digital Form Filling:

- Pre-filled application is presented to the customer based on existing KYC.
- Customer selects:
 - Customer Type (Individual/Firm/etc.)
 - Purpose (ReKYC due / Inoperative account/DEAF account/)
- Displays existing OVD details (Aadhaar, PAN, Address).

d) Document Validation:

- Aadhaar address and PAN validated via integrated APIs (UIDAI and NSDL/Income Tax).
- If no change in address or identity or in KYC documents, customer confirms via checkbox + OTP-based e-consent.

e) Submission & Update without VKYC (No Change Scenario):

- If validation succeeds and no update is needed, customer submits the journey.
- System auto-updates CIF records in the core banking system.
- Confirmation sent via SMS/Email.

f) Choice of Verification Mode:

- After form initiation the customer may opt to choose and or switch to any one of KYC verification modes:
- Video KYC (VKYC) – Remote Self-Service
- Digital KYC (DKYC) – Branch Official Assisted via Tablet/Device
 - VKYC/DKYC officer initiates session
 - Customer shows new OVD/address proof /PAN etc. live
 - Bank officials will be able to view the existing data including customers signature and changes requested by customer
 - Liveliness check, face match, session recording
 - Approval leads to ReKYC completion and CIF update and Inoperative status updating

5.4 Functional Requirements

- Platform Compatibility:
 - Responsive digital form on mobile, tablet, web
- Dedupe API Integration:
 - Identify existing customers via mobile number

- Pull latest KYC details from CBS
- CKYC, Aadhaar & PAN Validation:
 - CKYC search and download with auto pulling of CKYC data and PDF,
 - UIDAI Aadhaar authentication (address match, QR/Offline XML/eKYC)
 - PAN validation via Income Tax/NSDL APIs
- Change Detection Logic:
 - Compare existing address /KYC with Aadhaar address /KYC submitted with p
 - Prompt for VKYC/DKYC only when update required
- Digital Consent & Declaration:
 - OTP-based eConsent for no-change submission
 - Consent capture and archiving as per KYC norms
- VKYC Session Workflow:
 - Real-time video call
 - Session recording, liveness, geo-tagging
 - Officer approval interface with comments
 - CIF and activation of account auto-updated post-approval

5.5 Security & Compliance

- Aadhaar masking and secure deletion post-validation
- End-to-end encryption (TLS 1.2 or higher)
- RBI KYC Master Directions compliance
- Audit trail for every action
- Secure access for VKYC officers (AD/HRMS integration + OTP)

5.6 Integrations Required

- Core Banking System (CBS) for CIF validation & account update
- UIDAI for Aadhaar validation
- NSDL/IT APIs for PAN validation
- Notification systems (SMS/Email)

Note:

Any requirements before UAT sign off will not to be considered as CR. Any changes as per regulatory requirements not to be considered as CR, they shall be implemented at no additional cost to the Bank.

Table 2 - Journeys in the Scope

Sl No	Item Description	Variants / Number of Variants
1	VIDEO KYC – CIF OPENING	PERSONAL
2	VIDEO KYC – CIF OPENING	NON-PERSONAL
3	VIDEO KYC – SAVINGS ACCOUNT (Single & Joint)	5
4	VIDEO KYC – CURRENT ACCOUNT – INDIVIDUAL & SOLE PROPRIETORSHIP	2
5	VIDEO KYC – CURRENT ACCOUNT –	1

	PARTNERSHIP	
6	VIDEO KYC – CURRENT ACCOUNT – LLP & TASC	2
7	VIDEO KYC – CURRENT ACCOUNT – SHG	1
8	VIDEO KYC – TERM & RECURRING DEPOSIT (Single & Joint)	10
9	VIDEO KYC – NRE and NRO SAVINGS ACCOUNT (Single & Joint)	2
10	VIDEO ReKYC	
11	VIDEO KYC – PENSIONER LIFE CERTIFICATE	1
12	VIDEO KYC – BANKING CORRESPONDENT (BC) ASSISTED MODEL	1
13	VIDEO KYC – DIRECT SELLING AGENT (DSA) ASSISTED MODEL	1
14	VIDEO KYC – PPF, SSY & SCSS (Single & Joint)	3
15	VIDEO KYC – 3-in-1 SAVINGS ACCOUNT	1
16	DIGITAL KYC – CIF OPENING	PERSONAL
17	DIGITAL KYC – CIF OPENING	NON-PERSONAL
18	DIGITAL KYC – SAVINGS ACCOUNT (Single & Joint)	5
19	DIGITAL KYC – NRE & NRO SAVINGS ACCOUNT (Single & Joint)	2
20	DIGITAL KYC – CURRENT ACCOUNT – INDIVIDUAL & SOLE PROPRIETORSHIP	2
21	DIGITAL KYC – CURRENT ACCOUNT – PARTNERSHIP	1
22	DIGITAL KYC – CURRENT ACCOUNT – LLP & TASC	2
23	DIGITAL KYC – CURRENT ACCOUNT – SHG	1
24	DIGITAL KYC – TERM & RECURRING DEPOSIT (Single & Joint)	10
25	DIGITAL KYC – NRE and NRO SAVINGS ACCOUNT (Single & Joint)	2
26	DIGITAL ReKYC	1
27	DIGITAL KYC – PENSIONER LIFE CERTIFICATE	1
28	DIGITAL KYC – PPF, SSY & SCSS (Single & Joint)	1
29	DIGITAL KYC – 3-in-1 SAVINGS ACCOUNT	1
30	DIGITAL KYC – eKYC	1

Note: *

As per Banks business requirement Item or Variant may vary. Bank will have discretion to add and/or replace existing variant /product. The above journeys include different customer constituents like Personal & non-personal and Single & joint accounts.

B. Technical Scope of Work:

Module	Sub-modules
Architecture & Performance	1. Architecture
	2. API enabled
	3. Backup & Recovery
	4. Integration
	5. Logging
	6. Performance
	7. Solution Design
	8. Information Security
Security	9. Administrative Support & Monitoring
Support & Monitoring	10. Alerts & Notifications
Enabling features	11. Master Data Management
	12. MIS Reports, Query and Reporting
	13. User Management
	14. Workflow

Module 1: Architecture

Sr No.	Technical Requirements
1.1	Solution should have a modular design enabling addition of new channels or product lines, functionally scalable, flexible architecture. The application should be built preferably on micro-services architecture with API / message based inter module integration to support selective scalability, component level deployments and upgrades.
1.2	System to support minimum three tier architecture- Web server, App server and Database etc.
1.3	System should be able to comply with existing regulatory authority (RBI/IBA/SEBI/Government/etc.) requirements as well as flexible to handle future such requirements that may get published.
1.4	System should be highly parameterized to support the implementation of the bank's policy requirements and statutory policy requirements e.g., Future changes proposed by the monetary authority about timings of process, limit of process, normalization etc.



1.5	Solution with its all components must be deployed as per Bank's requirement at all existing and future Data Centers, including but not limited to DC and DR. The solution should be deployed with high availability for DC and DR site. The High Availability architecture may span across multiple Data Centers. Solution should support DC and DR to be run in active-active mode if required.
1.6	Solution should have modular design enabling addition of new channels or product lines or loosely coupled architecture based on micro-services pattern to provide flexibility in terms of quick feature/functionality releases and reduced time to go live.
1.7	System should support fault tolerant architecture with respect to software, hardware, network, etc. to prevent crash of system leading to its unavailability.
1.8	Solution Architecture should be flexible to enable customization or new feature/ functionality development that are specific to the Bank.
1.9	Solution must be highly configurable and must provide capability for the Bank to configure products and workflows which can be bundled into packages and deployed.
1.10	The solution must handle a minimum of 100 TPS (Transactions per second).
1.11	Solution should be designed for Cloud Native architecture to be deployed on premises at Bank's DC & DR. Solution should support containerized deployment.
1.12	Solution should be deployed on Bank provided RedHat Open-shift container platform and RHEL VMs based on IBM S390X architecture.
1.13	Solution should provide or support Cache services
1.14	Solution should provide or support Queue services
1.15	Solution should provide or support Auto scaling
1.16	Solution should provide or support Load Balancing services
1.17	Solution should provide or support API / Call Throttling
1.18	Solution should provide or support Batch processing
1.19	Solution should provide or support Message routing & transformation
1.20	Solution should provide or support Integration with API Gateway
1.21	Solution should preferably provide a Low-code No-Code platform to enable Bank IT team to introduce features and functionality for various journeys without the need to code.
1.22	Solution should support horizontal and vertical scalability.
1.23	Flexible architecture that is easy to configure, change and integrate into Bank's IT ecosystem. New functionalities should be added without impacting existing configuration & integrations.
1.24	Solution should have a parameter-driven product and workflow configuration to onboard new products with minimal code changes.
1.25	Solution should have a support for future integration with AI/ML-based modules (e.g., advanced fraud detection, customer segmentation).

Module 2: API Enabled

Sr No.	Technical Requirements
2.1	Comprehensive APIs for integrating with CBS or any other system for fetching/ updating information on real time basis.
2.2	Access to developer portal of vendor should be provided to bank to enable basic customizations/ tweaking of the available APIs.
2.3	Parameters of API should be configurable, means ability to tweak API based on Bank's requirements.

Module 3: Backup & Recovery

Sr No.	Technical Requirements
3.1	The system should allow having a day-end back-up process.
3.2	The system should also have recovery features in case of system failures.
3.3	Backup should be possible in external media tapes for off-site storage.
3.4	Online Backup and Real time replication of data should be available between DC and DR site. Databases at all data center sites should be in sync.
3.5	The Data replication should happen from Primary site to all DR sites on real time to keep them synchronized. In case of Solution running from DR the data replication should happen from DR site to DC on real time basis. Expected performance metrics in case of disaster : RTO (Real Time Objective): 2 hours, RPO : Near Zero.
3.6	The solution proposed should ensure regular backup on both online and offsite locations as decided by Bank.
3.7	Backups taken must be periodically tested via recovery option to ensure prevention of loss of data.
3.8	Backups taken in offsite location must be preserved in a secured location with access only to bank's authorised personnel.
3.9	No data would be purged. Server Data: All files and logs to be kept as per bank policy. Option for Archival & Purging should be available. Archived data should be made available through Bank's Object Storage and tapes.
3.10	System should support automated archival of data as per bank policy. System should support recovery of archived data for audit or investigation purpose.

3.11	Restoration testing from back up media and DR drills to be performed every quarter as per Banks Schedule.
------	---

Module 4: Integration

Sr No.	Technical Requirements
4.1	Solution should allow for Integration with CBoI internal and 3rd party external systems etc. via Industry standard approaches like Custom Adapters, RESTful API, etc. These integrations can be a) allowing access to DKYC & VKYC APIs or b) DKYC & VKYC making calls to these systems. Key aspect of all functionalities to be supported on Mobile App and need to be available through RESTful APIs with JSON.
4.2	System should support data exchange with all the channels i.e. web upload, email, SFTP, H2H, web service /API, form based, Bulk and batch process for file transfer and future technologies channels etc. should be able to segregate different modes of processing as per the defined data.
4.3	As part of file handling, System should be able to split /generate/control the file, in case of manual upload to desired limit as per user's requirement.
4.4	System should be capable to Integrate with third party APIs
4.5	System should integrate with Banks's mail systems to generate notification on mails and SMS and through auto mailers.
4.6	System should integrate with Payment gateways for the initial deposit collections.
4.7	System should integrate with Bank downstream systems like CBS, Omnichannel App, Digital lending platform etc.
4.8	System should integrate with Bank's internal systems like ADS (Employee SSO), Monitoring Applications, SIEM, DAM, SOC, PIMS, Data Warehouse, DLP, Antivirus, APM, Application Whitelisting etc.
4.9	Application should integrate with other applications like existing gateways of RBI, IDRBT, NPCI, GST, FinTech's, ONDC etc.
4.10	Solution should host APIs viz. API (REST-Bulk) API (REST-RealTime) API (SOAP-Bulk IDOC PEXR2002 format) API (File Upload)

Module 5: Logging

Sr No.	Technical Requirements
5.1	The system should generate error which should be descriptive enough to allow traceability of the data/function error to the most granular level as per Bank's policy.
5.2	System should allow configuration-based start/stop of logs based on levels (Information/Warning/Error/etc.). These should be descriptive enough to allow traceability of the data/function error to the most granular
5.3	Confidential or PII (Personally Identifiable Information) data in log should be adequately encrypted, tokenized, masked as per Bank's policy.
5.4	Solution should provide comprehensive configuration-based event logging for monitoring, auditing and troubleshooting purposes as per Bank's policy.
5.5	All logs should be maintained for each action taken with timestamp, unique ID, Trace ID, user ID and IP address
5.6	Audit Logs for all Upstream & Downstream systems should be maintained as per Bank's policy.
5.7	Audit trail for actions performed by information security administrators (at security module level) as per Bank's policy.
5.8	Logs for any modification done should be available with the required details for audit as per Bank's policy.
5.9	Audit trails should contain sufficient details to reconstruct events to determine the cause of the security violation or malfunction as per Bank's policy.
5.10	Application should not allow any amendments/deletion to Audit Trails, Transaction Journal and Logs.
5.11	Logs should be maintained at every level of the application layers as per Bank's policy.
5.12	User related activities including successful and unsuccessful attempts to sign in must be recorded in the log files.
5.13	Audit trails should be recorded for all activities including financial and non-financial activities at application level, DB level, Middleware level, OS level etc.
5.14	Application logs to be integrated with Security Operations Center (SOC) for monitoring purposes as per format defined by SOC.

Module 6: Performance

Sr No.	Technical Requirements
6.1	System Uptime should be minimum 99.95% per day.
6.2	For the web application the static page load time (e.g., Login page) : < 2 secs
6.3	Rendering Search results on the web pages should be < 5 seconds
6.4	Rendering MIS reports or Dashboard should be <5 seconds.

6.5	Application Programming Interface (API) response time should be: Asynchronous API Calls < 2 seconds. Synchronous API Calls < 1 second. These are APIs that are built and hosted by the Platform.
6.6	Transaction failure due to technical reasons below 0.01%

Module 7: Solution Design

Sr No.	Technical Requirements
7.1	Access to application API from Corporate/Government would be via secure authentication e.g. TLS, Encryption, Digital Signature, Tokenization etc. As per Bank's policy guidelines time to time without any development / additional cost to the bank.
7.2	Solution should be Web Application compatible on all latest versions of major web browsers- Microsoft Edge, Google Chrome, Mozilla Firefox, Safari etc. and on mobile application without any development / additional cost to the bank.
7.3	Web applications to be built are DKYC, VKYC, PLC & ReKYC
7.4	The solution interface should support adaptive design based on various form factors available in Desktops, Laptops, Smartphones, Tablets, etc. which would be used by the end users of this application as per Bank's design guidelines.
7.5	Solution would have web portal-role based access for Bank Users: Super Admin, Admin, Marketing Executives, RMs, Central Office users, Branch Maker, Branch Checker, MIS/Report User etc. Agents: A) VKYC Handling agents. B) VKYC Auditors C) DKYC Makers D) DKYC Checkers The application and workflow should be customized as per Bank's requirement.
7.6	The system should generate standard custom defined error messages based on pre – defined parameters.
7.7	End-users would see business friendly messages while the actual error message should be made available to IT team for Root Cause Analysis (RCA) purposes.
7.8	Solution should have Bank's branding in terms of logo, color schemes, fonts and other branding content on the channel etc. as per Bank's design guidelines
7.9	The system should be capable of displaying the details of corporate, Government body's logo, name, address on the portal as part of personalization.
7.10	It should support data entry via upload of files in various industry specific standard formats like ZIP, RAR, PDF, XML, IMAGES (JPG,JPEG, TIFF, etc.), EXCEL, DOC(x), TXT (Delimited & Fixed length), CSV, DAT, ISO 20022 etc. centrally or from Corporate/Government/banks location etc.

7.11	System should support file formats with headers, footers and blank lines or without headers, Footers and blank lines, with any delimiter as required by clients
7.12	It should support ISO8583 messaging formats etc.
7.13	System should have user-friendly and intuitive interface as per Bank's design guidelines
7.14	Access to the solution for Banks employees should be from Banks Intranet / VPN / MDM, TAB, Mobile devices.
7.15	For devices to be used for access by Bank Employees (via Intranet access), Solution should support Office connected desktop/Laptop, TAB, Mobile, MDM connected devices etc.
7.16	For devices to be used for access by Corporate/Govt. users. (Via Internet Access.), Solution should support Desktop/Laptops/Smartphones from Internet or via VPN access. Additionally, access via H2H / SFTP /API/ Dedicated connections/etc. also must be provided. The Architecture design should support them.
7.17	Version Control and rollback Mechanism should be implemented to track both product versioning as well as the custom design that gets released to production. Solution should integrate with Bank's DevSecOps platform for Versioning and CI/CD deployment, Project Management, Container Registry and Security Scans.
7.18	Proposed solution should have integration with Bank's Omni-channel Platform.
7.19	System should ensure processing of unique transactions only so that no transactions are processed twice.
7.20	The system should be capable of displaying advertisement and marketing banners on the portal - On login page and on landing page post login.
7.21	Solution should have file Format Mapper - Ability to define & map file formats (input file as well as response file) as per customer's unique requirements.

Module 8: Information Security

Sr No.	Technical Requirements
8.1	Secure coding practices should be used. Please refer NIST SP 800-204C or the latest one for detailed guidelines on Microservice based architecture
8.2	NIST SP-800-190 (Application Container Security Guide) should be followed for Microservice based architecture
8.3	If source code is not shared with bank, then Vendor to provide latest Security Review Report done by any CERT-IN empaneled ISSP
8.4	Application should be tested and patched against known vulnerabilities as defined in OWASP Top 10 and SANS 25 prior to handover to the Bank.

8.5	No static details regarding project (e.g., Default username, password) are mentioned in the code.
8.6	Obfuscation of code to be done while putting the project into production.
8.7	DevSecOps activities and processes should be followed and aligned with SDLC (Software Development Lifecycle) framework in Agile mode and IT service management processes (e.g., Configuration management, change management, software release management). Bank's DevSecOps platform should be used for the above activities.
8.8	Transfer of software from development to test and test to production should follow a controlled procedure to ensure that only the software that has undergone testing can be released to production. Bank's DevSecOps platform should be used for the activities.
8.9	Adequate knowledge transfer should be planned. Knowledge transfer includes but not limited to transfer of skills, operating processes, and procedures. Focused training sessions, handholding for certain period and detailed documentation should be used to ensure knowledge transfer. Reverse Transition Plan should be made available.
8.10	Vendor to support DevSecOps Implementation using Bank's DevSecOps Platform to ensure that Deployment/Rollback in production would be automated without the need for access to servers for Vendor.
8.11	The software solution should follow best practices in architecture, design and coding. In the case of web application, it must adhere to OWASP design and security guidelines.
8.12	System should support Single Sign-On (SSO). Single Sign-On would have to be with the Active Directory Services (for Employees). Single login and single reference ID (corporate ID) for all modules and single sign on Omni-Channel.
8.13	The PII data should be stored in encrypted form. It should have capability for data encryption, tokenization and masking. Movement should also happen in encrypted form.
8.14	The data should be stored in encrypted form as per Bank's policy.
8.15	Movement of data should also happen in encrypted form as per Bank's policy.
8.16	Solution should have capability for data masking, encryption, tokenization and data vaulting etc..
8.17	Users should be able to change their passwords for login/ transactions without manual intervention. This process must be secure with Multi- Factor Authentication (MFA)
8.18	Bank users would follow the existing policy on password changes as it would be integrated with their employee account in Active Directory.
8.19	Support two/multi factor authentication mechanism during login e.g. OTP, Biometric , Tokens /Soft Token/Hard token or any other secure way of login
8.20	Role based access to the system should be available.



8.21	System should be deployable on secured and hardened infrastructure including Application, OS, Database, load balancers, web logic implementation via middleware (e.g. web servers Tomcat, WebSphere etc.) as per Bank's policy
8.22	System to support Virtual keyboard option during password entry during corporate login.
8.23	The Unsuccessful attempts to log-in to the system should be recorded on the log files.
8.24	Verification of identity of users through User Id/ Passwords (As per banks password policy & in encrypted format).
8.25	Solution should support Mechanism of Multifactor Authentication of Transaction Authorization – OTP, Biometric, Transaction password, Tokens /Soft Token/Hard token, or any other secure way of authorizing transactions
8.26	It should check/record/verify authentication of source of each transaction like user IDs, IP address, Mac address etc. and maintain logs which is required for AUDIT purpose.
8.27	Data entry / upload of files should be with due authentication and encryption
8.28	Support for file upload with digital signature/ RSA token/ encryption.
8.29	Option for Two or more users should authorize file upload, with provision for multi-level authorization for bulk/individual uploads depending on Bank's requirement (e.g., Multilevel authorization for amount exceeding a ceiling limit). Maker checker concept should be present.
8.30	System should support forgot password retrieving facility.
8.31	System should support inactivity period number or retries for login feature, last login time, session time, out time, idle time etc. as per Banks policy.
8.32	System should support CAPTCHA authentication.
8.33	Movement of data (in Transit) should be secured and encrypted via TLS 1.2 and above
8.34	System should support security features such as SFTP, HTTPS, Digital Certificates etc.
8.35	System should support security features such as encryption, decryption, hashing, salting, signature verification etc.
8.36	System should support security features such as digitally signed data transmission and verification.
8.37	Different levels of authorization should be available. System should be capable to allow users to access /create/ modify object or functionality as per their roles.
8.38	System should support TLS1.2 and above certificate and as per Bank's policy on time to time

8.39	System should adhere to any data related requirement as prescribed by the regulator, government or Bank from time to time. This adherence should not result in any cost impact to the bank.
8.40	System should have auto log-off functionality on session timeout or user inactivity, idle timeout etc. as prescribed by the Banks IS policy.
8.41	The solution should provide H2H integration with encryption, decryption and digital signature with corporate ERP/ other operating systems for secure file transfer between the corporates and the Bank. Encryption algorithm of client should be supported by the system.
8.42	Architecture should ensure the security of the deployment architecture by segregating the servers into various security zones, e.g. Web Server in DMZ, App Server in MZ, Database in Core MZ, etc.
8.43	Any type of Remote access to the system outside the Bank's network will not be allowed.
8.44	Proposed Solution should integrate with Bank's existing Aadhar Vault to store and retrieve Aadhar Numbers.
8.45	System should support IPv4 & IPv6 protocols.
8.46	Data at Rest: Application Logs: To be encrypted. PII (Personally Identifiable Information) data should be masked. Log structure should be as per CBOI guidelines. Database: TDE (Transparent Data Encryption) & Redaction to be implemented, PII Data stored in Database should be in encrypted format, encryption and decryption should be taken care by the application in real time. All passwords/PINs: should be hashed with Random salt at the time of input. Minimum: SHA-2 or equivalent and above
8.47	Data in Transit: Channel level security TLS 1.2 and above in all communications including Web to App to DB server. All File based communication to have additional encryption on file. API communication should have payload encryption in additional to authenticated access. No sensitive/PII data should be visible/in plain text during the whole communication including internal communications.
8.48	API Integration: Authentication: Token based, Symmetric/Asymmetric encryption, hashing Payload: Payload Encryption.
8.49	Application should support Bank's Password policy .
8.50	Access of the solution for other systems (Internal/external) would be via authenticated and secure API calls.
8.51	Access to the infrastructure hosting the solution would be via restricted, authenticated access through Privileged Identity Manager. This access would be available only from the Bank's IT Centers and on Bank Network. Test, Pre-prod environment: Access to Vendor and Bank IT teams. Production (and DR): Access would be given to Access to Vendor Support team and

	Bank IT Teams
8.52	Open source software components will not be considered in the solution. All components should be with enterprise license and highest level /Grade of 24X7OEM support. For the entire contract period of 5 years.
8.53	The software should be supplied with enterprise license only. Community edition/open licenses will not be accepted by the Bank.
8.54	All credentials regarding the application solutions like Application, Database, OS passwords etc should rest with Banks Authorised personnels only.
8.55	The solution must be integrated with Bank's Active Directory using LDAP.

Module 9: Administrative Support and Monitoring

Sr No.	Technical Requirements
9.1	System should have facility for monitoring all files & transactions for customers and Ops team. The system should be monitorable at component level and required telemetry (observability), logs available for quick response & resolution in defined SLAs.
9.2	Community editions of any components are not allowed even if supported by the bidder.
9.3	User administration Module for managing user accounts, defining roles and rules, workflow, Monitoring of user activities.
9.4	Define workflow for various system activities through setting parameters through front end.
9.5	Managing and Monitoring of system resources like storage, usage and likewise.
9.6	Version maintenance, change management and tracking of Application, Scheduling back up of application.
9.7	Maintenance of UAT environment. UAT set up should be in synchronization with live application in terms of Database structure and functionality.
9.8	Module for tracking change requests.
9.9	Audit trails should be enabled for all activities including financial and non-financial activities.
9.10	Logs for all/any modification done should be available with the required details for audit.
9.11	Audit trails should contain sufficient details to reconstruct events to determine the cause of the security violation or malfunction.

9.12	Application should not allow amendments/ deletion to Audit Trails, Transaction Journal and Logs.
9.13	The application should have the master maintenance module along with the owner (creator, verifier, checker, administrator and viewer role).
9.14	The bidder should provide a mechanism to monitor the Database.

Module 10: Alerts & Notification

Sr No.	Technical Requirements
10.1	System should be able to provide internal notification for action item, pending authorization, final authorization to authorized users/approvers etc.
10.2	System should support notification through various modes such as email, SMS etc. automatically as per banks requirements. This notification can be to internal (bank) or external (Customer/Agency/etc.) users etc.
10.3	System should support E-mail and SMS alerts for Exceptions.
10.4	System should be able to integrate with Bank's downstream applications like Core Banking Solution, Integrated Payment Hub (IPH), Executive Information System (EIS), Bank's API Gateway, APM tool, Aadhaar Data Vault (ADV), Enterprise Service Bus (ESB) etc. on real time basis to pull data for giving alerts/ notifications
10.5	Alerts on specific transactions based on events. This should be customizable and should not require code level changes and redeployment. (e.g., broadcasting message for shift to DR)
10.6	Alerts (SMS & email) & notifications on transactions, creation, renewals, inactive customers etc.

Module 11: Master Data Management

Sr No.	Technical Requirements
11.1	System should have Master Data Management module with Maker-Checker functionality and audit trail around it.
11.2	System should be having functionality for creating and maintaining Customer/ Bank/Branch and any other Masters (Data entry and File upload system etc.).
11.3	Master Data module should be loosely coupled with the system so that any additions/updates to master data need not require solution redeployment
11.4	System should be capable of defining the charges at client level/product level at various frequencies like monthly/quarterly/yearly etc.

11.5	System should have ability to define holidays, day begin and day end facility. System should be capable of maintaining Holiday masters: national / state / district / branch / day wise.
11.6	Capability for client master creation with all KYC compliance. System should be capable of maintaining client wise authorization / escalation matrix.
11.7	Customer master should support single account, multiple account, limits for each account and charges.
11.8	System should have the ability to bulk upload for creating Users, Group creations, Authorization mappings, maintain list, create rules, Account linking etc.
11.9	System should have bulk uploading functionality to upload customers data files like LEI master etc. with modification / deletion or addition etc.
11.10	System should have the ability for modification/addition of multiple accounts in existing group at one go.
11.11	The DKYC & VKYC should be able to maintain or fetch master data from CBS or through any upload. The following master shall be maintained: a) Bank and Branch masters (through manual entry/file uploading) along with location master b) Account, Product master c) Authorization and Escalation matrix d) User master e) User role definition master with upgrade and downgrade of user f) Holiday master's maintenance (national / state / district / branch / day wise) for admin users. g) Product set up parameters should be configurable through front end.

Module 12: MIS, Query and Reporting

Sr No.	Technical Requirements
12.1	System should support schedule-based generation and mailing of various reports through scheduler and auto mailer as per banks requirement.
12.2	Allow users to export MIS reports in standard formats like Excel, PDF, TXT, CSV, XML, JSON etc.

12.3	System should have facility to enable Bank to login and download MIS reports required by them over WEB, API, Email, SFTP, H2H etc.
12.4	The system should allow users to download and print reports directly from their login.
12.5	There should be provision to send variety of reports through AUTO MAILER and on required frequencies
12.6	Provision to send similar type of reports to specific group through auto mailer. Parameterization required for selection of auto mailer reports.
12.7	Exception reports should be available.
12.8	Application should have basic reporting options and should have report building flexibility to users. Facility to design reports as per requirements. Report writer/builder should be available to the Bank to generate their own reports and queries.
12.9	System should support various hierarchy-based reports like Branch manager should have access to his branch report and Regional Office, Zonal Office, Central Office have access to overall reports etc. rule and role based.
12.10	Interface with Drag & Drop/mapping of fields option to create dynamic MIS formats based on the requirements from different clients. Since requirements will be different from client to client, defining of MIS formats can be easy for various requirements from clients.
12.11	System should provide separate, incremental, cumulative, consolidated MIS etc. for collection as well as payments in the format required by client.
12.12	MIS Module should support all latest security algorithms like Digital Signature, PGP etc. for encryption and decryption of files.
12.13	MIS reports can be viewed across various devices like mobile, laptop, desktops and tablets.
12.14	MIS and databases should be readable via third party tools like Tableau, R, Power BI, Python, SQL Developer etc. and exportable in csv, txt, xml etc. formats for running analytics.
12.15	MIS and Real time reports generation should be possible from DR servers.
12.16	System should enable monitoring of all transactions and files both at bank end. System should support monitoring of processing engines and related integrations
12.17	The application should be integrated to Bank's mail server & SMS server for sending the generated MIS through auto mailers / auto SMS.
12.18	The application should be configurable to fetch data from various platforms through API for generation of various reports.

12.19	The files generated from DKYC & VKYC application in the form of MIS reports should be non-tamperable within the Bank and at client end.
12.20	Application should have basic querying options and need to be customized based on the products/ processes defined by the Bank.
12.21	Application should provide multiple initiation modes, query for areas including real time status, real time alerts and notifications and download reports.
12.22	Application should have basic reporting options and should have report building flexibility to users.
12.23	It should have the facility to design the reports as per the Bank's requirements.
12.24	System should enable the user to view the full details of a customer. Account aggregation – one view account summary of all accounts in a single or multiple report.
12.25	The notifications must be customizable by the Corporate as follows – a) Text of the message b) Incorporate variable data from DKYC & VKYC transaction tables c) Channel for delivery - email, SMS or WhatsApp, as required

Module 13: User Management

Sr No.	Technical Requirements
13.1	User Management Module to be available for Bank. With audit trail capability.
13.2	Role based access to be supported for customers which should be configurable.
13.3	Addition/ management/ activation/ deactivation/ reactivation/ modification/ deletion of user profiles- internal roles (bank) and external roles (customers)
13.4	Bank can administer and manage user creation and profiles, roles and workflow rules for their respective entity.
13.5	Multi users with granular access controls/ entitlements and work flow management
13.6	User management options like lock, unlock, reset login password etc.)
13.7	Support organization hierarchy, user, role based access with proper authentication and audit trails
13.8	System should provide features for disabling a user, temporarily suspending rights to a user and automatic deactivation of user in case of inactivity for a defined period.
13.9	System should have the ability to upgrade and downgrade the user.

13.10	System should have the ability to import currently onboarded data/old data of customers.
13.11	User administration Module for managing user accounts, user groups, Defining roles and rules, approval workflow and monitoring of user activities.
13.12	System to identify user type basis login credentials and route to respective landing page (maker, checker, authorizer)
13.13	Authorized users to perform transactions on the selected account up to the specified transaction limit
13.14	User management and access rights configurations should be supported by way of individual users or group of users for records or file uploads

Module 14: Workflow

Sr No.	Technical Requirements
14.1	Define workflow for various system activities through setting of parameters through front end.
14..2	System should have a workflow which provides flexibility of Multi- level/ Sequential/ Parallel/ Quorum based approval workflow rule definition. These should be configuration based.
14.3	Bank Users should be able to define workflow, queues and priorities based on various criteria, such as queue for items needing manual intervention with proper notification, if item in queue is awaiting or exception has occurred

11. Software License

Sr. No.	Technical Requirements
11.1	Bidder should provide perpetual Licenses for Data Centre (DC) setup, Disaster Recovery Centre (DRC), NDR, UAT & Pre prod setup for unrestricted use across the organization viz. Branches, Location & clients irrespective of locations or number of users.
11.2	All software envisaged is required to be on-premises irrevocable perpetual software licensed to Bank, right to use the software even after the contract period. Only licensed copies of software shall be supplied and ported. Further, all software supplied shall be of latest version and will be upgraded with functionalities from time to time.
11.3	The Solution must be web and mobile based, user friendly and the application should work using low bandwidth and high latency. The solution should work seamlessly for customers of the Bank and all related Bank Branches irrespective of location.

11.4	The solution should be in High Availability at both DC & DRC virtualized. Database should provide High availability & disaster recovery with a cost effective and optimal solution.
11.5	In the event of the bidder being not able to perform the obligations as per the provisions of the contract, the OEM/OSD/principal should assume complete responsibility on behalf of the bidder for providing end-to-end solution i.e., technology, personnel, financial and any other infrastructure that would be required to meet intent of this RFP at no additional cost to the bank. To this effect bidder should provide a certificate duly signed by OEM authorized signatory for the proposed solution.
11.6	Bank reserves the right to modify the scope due to change in regulatory instructions, market scenario and internal requirement within the overall objective of implementation of DKYC & VKYC .
11.7	During the project, there might be related areas which Bank would like the selected Bidder to undertake which may not have envisaged earlier. Bank reserves the right to pause the work at any point of time and use the services for partial delivery of select modules of the Solution.
11.8	The Installation will be deemed as incomplete if any component of the Solution is not delivered or is delivered but not installed and / or not operational or not acceptable to the Bank after acceptance testing/ examination. In such an event, the supply and installation will be termed as incomplete and system(s) will not be accepted. Installation will be accepted only after complete commissioning of Solution.
11.9	The solution will be accepted after complete integration and satisfactory working of the solution.
11.10	The selected Bidder must work with different application vendors to integrate new solution to the existing workload or new workloads during contract period with no additional cost to the Bank.
11.11	The selected Bidder has to work with different teams of Bank, customers of Bank & application OEMs to understand the policies requirement and configurations of respective applications for the offered solution.
11.12	If contract further extends, bidder should have back-to-back agreement with the OEM/s for further renewal of support services. Undertaking should be submitted duly signed by Bidder & OEM in this regard.
11.13	DKYC & VKYC Solution should have the capability to be integrated with Bank's Omni Channel platform & any other existing / future banking application procured by Bank.
11.14	Selected bidder should be providing the middleware/API to connect Client's ERP Solution and Bank API Gateway.
11.15	Selected bidder must maintain, manage and provide API inventory in Open API specification format to cater to our core DKYC & VKYC requirements.
11.16	The selected bidder shall provide the Bank, understanding and full access to database, database table structure and data dictionary of the proposed solutions.

11.17	The selected bidder will be responsible for customizing, testing and maintaining all the required interfaces during the contract period at no extra cost to the Bank. In case of any subsequent change, modification or alteration to the Bank's existing Application software packages, the Bank will obtain the API for such existing Application and provide the same to The Bidder for interface at no additional cost. The Bank has envisaged all the interfaces to be on an online secure mode with Straight through Processing.
11.18	The selected bidder will ensure and incorporate all necessary security and control features within the Application, operating system & database to always maintain integrity and confidentiality of data.
11.19	The selected bidder will be responsible for creating an exhaustive set of UAT test cases. The selected bidder will provide dedicated resource for same. Bidder shall ensure that the test cases meet all the testing requirements of the Bank. The Bank will review the same and may propose additional test cases.
11.20	The selected bidder to engage an independent 3rd party with experience of conducting UAT for the proposed solution in a Scheduled Commercial Bank in India to conduct testing followed by System Integration testing and assist the user in carrying out User Acceptance testing.
11.21	The selected bidder or 3rd party are responsible for preparing detailed test cases and test cases repository. The selected bidder needs to conduct SIT and UAT on manually created data at first followed by on Banks data in the Banks Environment.
11.22	The selected bidder or 3rd party are expected to assist the Bank in conducting all the tests and analyzing /comparing the results. The selected bidder shall provide full-time resources conversant in all business areas, for troubleshooting during the entire UAT process.
11.23	The Bank has a right to interview and reject resources before boarding. (The deviation of >10% in Effort Estimate for any development and or new requirement from the bank will attract appropriate penalty in cost estimated.) Facility Management team should be available on-site and would resolve day-to-day production issues reported on all applications by debugging and analyzing the same.
11.24	The OEM may from time-to-time release Updates/ Upgrades/New releases/New versions and notify the Bank about the same. The Bidder agrees that all such Updates/Upgrades/ new releases/New versions, as and when released during the contract period will be implemented without any additional cost to the bank.
11.25	Bidders have to note that Support for IPv6 is required as recommended by RBI Guidelines. This is applicable for the entire Solution proposed by the Bidder as part of the RFP. Also, the Bidders should ensure that the Solution should be compatible to IPv4.
11.26	Before live implementation / migration of the software solution in production system, the product may be audited by Bank's appointed Software Audit firm / in house team.
11.27	All audit points raised by the auditor internal, external & any other Regulatory Authority in their periodic audit should be complied with by the bidder within the stipulated timeline & without any additional cost to the Bank.
11.28	During warranty and ATS period, the bidder needs to comply with security and system audit observation without any additional cost to the Bank.

11.29	The Solution should have a compatible end to end IT architecture covering: I. solution architecture II. integration architecture III. implementation architecture
11.30	Bidder has to follow best practice and international standards for documentation for the entire system development life cycle. The documents and manuals should be kept up to date with proper version control and rollback during the entire contract period. Bank may require the bidder to deliver the following documents in hard and soft copy to Bank during development and implementation of the solution.
11.31	Detailed System Requirements Specification Document to be provided: a) High Level architecture document and Diagram b) High Level Design document and Diagram c) Low Level Design document and Diagram d) Test cases with results during UAT, SIT and any other test cases e) Deployment plan document and Diagram f) Change management methodology document g) Security guide h) User management guide i) Release notes j) Impact matrix Standard Operating Procedure document for all processes mentioned in this RFP.

12. Hardware Requirement

Sr. No.	Technical Requirements
12.1	The Vendor must provide necessary requirement of infrastructure in the format (Servers / Storage/ RAM/ Core (vCPU)/ OS / Database / Middleware which are required for the system) for DC, DR & UAT with proper justifications and evidences. All the servers requirements provided by Bank will be on S390X architecture. RHEL VM's and Red Hat OpenShift will be provided by the bank on S390X architecture. If the solution requires any other architecture, OS, Database or any Component, those hardware and software components and licenses need to be brought in by Bidder.
12.2	The Vendor must provide requirement of optimal size of the Hardware, operating System, Database, keeping in view the current average and peak volume of transactions and to extrapolate the same for the full contract period (i.e., 5 years). Some of the basic parameters (indicative) for sizing as per the annexure 14

12.3	Expected Application Response Time a) Static Page loading like login page - < 2 Seconds b) Executing search and rendering search result on application user interface - <5 Seconds c) Viewing of report of size <1 MB – 5 Seconds. d) Making transaction on the system report generation - <5 Seconds
12.4	Bank will provide necessary DB licenses (Bank will provide Oracle DB licenses only. If bidder proposes any database other than oracle DB, then the enterprise license same should be provided by the bidder and enterprise license cost should be factored in commercial bid), Backup infra, Load balancer, NW switch +IPS, WAF, DDOS Antivirus, any other security and Bank specific tool as per banks architecture.
12.5	The bidder needs to design & size the hardware required at DC, DR & UAT setup. The bidder is to provide the complete hardware requirement (under Hardware Sizing / Bill of Material) for the end-to-end functioning of the solution.
12.6	Bidder is responsible to arrive the sizing independently. The Bank is not responsible for any assumption made by the bidder not meeting the performance/service levels as desired. In such a case, the bidder will at their cost carry out the necessary upgrades /replacements. The hardware sizing submitted by the bidder must be sufficient to meet the requirement of the Bank during the contract period.
12.7	Bidder needs to factor the required infrastructure / Licenses in the bill of material. Bidder is responsible for the optimum sizing. Bank will provide hardware, OpenShift licenses, RHEL Licenses and Oracle DB on S390X platform, all other licenses should be provided by the bidder and the same should be factored in Bill of Material.
12.8	The bidder shall propose hardware sizing, the bidder to do Application fine tuning first without any additional cost to the Bank and if required, additional hardware can be augmented post fine tuning as decided by Bank
12.9	Bank will provide the licenses of OS (RHEL), Open Shift and database (oracle) on S390X only as mentioned above and no need to be factored by the bidder. Bidder need to factor the license details with proper and justified sizing required for proposed solution. All the dependent software/tools required for the application should be Enterprise version and required licenses should be provided by the bidder.
12.10	Supply and installation of required integrate DKYC & VKYC solution at DC, DR & UAT setup. All three environments should be deployed as: a. DC (HA) b. DR (HA) c. UAT/Development (20% of production in non-HA)
12.11	The solution should function across Bank's DC & DR on active-active / active – Passive mode as decided by the Bank.
12.12	The proposed solution will be deployed by bidder in a highly available manner such that the failure of a single server/node will not interrupt the running application.

12.13	DR capabilities or sizing should be provisioned or proposed by the bidder, allowing the entire environment to quickly be moved to a different physical location with a minimum visible impact to end-users. DR site will also be deployed by bidder with same architecture and same capacity as of production DC site.
12.14	The sizing of the non-production/UAT environments should be adequately sized. The architecture of non- prod environments should have similar architecture of production.

In case, the hardware to be provided by the Bank, the hardware will be on prem with S390X architecture on IBM LinuxOne Zsystems, Operating system – RHEL on IBM LinuxOne, Microservices / Container Platform – Red Hat OpenShift Container Platform, DevSecOps – GITLAB, Database – Oracle DB, Web Logic. Only Oracle License will be provided by the Bank, Installation, Configuration, Maintenance and Backup will be performed by the successful bidder.

The sizing of hardware / Software must be based on current average and peak volume of transactions, Oversizing of hardware and the same is under-utilized will lead to penalties.

13. Onsite Support:

The Bidder shall be responsible for providing adequate support for proposed DKYC & VKYC hosted at DC and DR during Contract period. The resources should be deployed at Head Office (or any location specified by Bank), for the entire contract period. The on-site support should extend to services like technical helpdesk, system backup, data backup, user management, database management / maintenance, application management, updating of data, maintaining integrity of data, loading application upgrades, technical support for ad-hoc queries, Performance Testing, archival of data and any other support required with respect of DKYC & VKYC application. Query/issue raising and escalation process system should be in place. Support should be provided for Complaints/Issues/Queries raised through Email, Helpdesk, CRM, etc. and resolution of issues as per TAT agreed in SLA between Bank and the Vendor. All the On-site resources shall be on the payroll of the bidder and not any third-party organization.

Minimum Resource Deployment during contract period

Type of Resources	Location	Number of Shifts per day (8 hours)	Minimum no. of resources Per Shift
L2	Head Office (or any location specified by Bank)	2	2
L2	DBA	1	1
Total L2			5
L3	Service on call basis, if required		

However, if needed, bidder can engage more resources to meet SLA, uptime and scope of work defined in this RFP during contract period.

Minimum Qualification for **Resources**

SN	Position	Proposed Skill Sets
1.	Level L2	Qualification: • B.Tech/MCA/M.Sc.(IT) Experience: Candidates who have minimum 3 years of hands-on experience in managing DKYC & VKYC Banking related Solutions of any reputed organization with at least 1 years' experience in managing VKYC / DKYC Solution in BFSI sector.
2.	Level L2 (DBA)	Qualification: • B.Tech/MCA/M.Sc.(IT) Experience: Candidates who have minimum 3 years of hands-on experience in managing Database of any reputed organization with at least 1 years' experience in managing Database in BFSI sector.
3.	Level -L3	Qualification: • B.Tech/MCA/M.Sc.(IT) Experience: Candidates who have minimum 5 years of hands-on experience in managing VKYC / DKYC Solution of any reputed organization with at least 2 years' experience in managing VKYC / DKYC Solution in BFSI sector. Skills: 1. Sound analytical and troubleshooting skills 2. Good Team Management and co-ordination skills

14. Training

Sr No.	Sub-module	Technical Requirements
14.1	Training	The Vendor shall organize for training to the Bank's team as follows: Vendor must impart training to the Bank's Core Team (2 batches of 20 people) (IT as well as functional) before UAT. The training should cover configuration, operation / functionalities, maintenance, support & administration for software / middleware, application architecture and components, installation, troubleshooting processes of DKYC & VKYC application.
14.2	Training	Training to the IT team should cover the system administration viz. - System Administration & User management - Management of Application software - Data base administration - Report writing - Security management - Backup & Disaster Recovery Operations - Troubleshooting - Creation of document category - Designing workflow - Management of servers, storage, database and security etc.
14.3	Training	Demo portal, SOPs, User manuals for training of all stakeholders-branch, customers & Ops team should be provided.
14.4	Training	Training on Development –Vendor to arrange for comprehensive technical training primarily on development of workflow solutions, report writing, dashboards on the following topics - Workflow solutions / Business Process Management - Integration between various programs / applications with solution - Linkage between various programs and modules of applications software Program coding

Adherence to Regulatory Compliance

The Bidder to ensure compliance:

- To RBI's Master Directions on IT Outsourcing 2023,
- RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2023,
- RBI Master Direction on KYC and related directions on Digital-KYC & V-CIP
- DPDP Act. & Rules
- Other relevant RBI's Master Directions and circulars issued and enforced time to time for managing service agreement, risk, security of application, security of process, security of data, privacy and business continuity.

- IT Act 2000, ISO 27001, ISO 22301, ISO 27701, SOC 2 Type II, CSA Star Level 2 Adherence to at least Level 3 of process capability levels under the COBIT 5 Process Assessment Model based on ISO 15504-2.
- Bidder to ensure compliance to all applicable ISO, RBI, SEBI and other statutory, regulatory and legal guidelines as and when in forced by the respective authorities.

15. Important General Terms & Conditions

15.1. Maintenance Support:

The Bidder must provide uninterrupted availability of the system and ensure that the problem is resolved within the time schedule as prescribed in the Service Level Agreement (SLA). Maintenance support will also include installation of system updates and upgrades, providing corresponding updated manuals, and follow-up knowledge transfer. During the AMC/ATS period, all upgrades should be free. All regulatory / statutory changes should be done without any additional cost to the Bank.

The bidder should be authorized partner of OEM and should be having back-to-back support of Original Equipment Manufacturers (OEM) for the components included in the proposed solution. The bidder should provide documentary proof on back-to-back OEM support. The back-to-back Support agreement with OEM should include the activities such as Technical Assistance support, Software upgrade support etc. on 24x7x365 basis.

Remote Connection from outside of Bank's network will not be allowed at any point of time.

The installation, re-installation, configuration, maintenance of the system software and application software, if required is the sole responsibility of the successful Bidder, which should be treated as service provided under Maintenance support.

15.2. ESCROW Arrangement:

The Bank and the Vendor shall agree to appoint an independent escrow agent to provide escrow mechanism for the deposit of the source code for the software product supplied/procured by the Vendor to the Bank to protect its interests in an eventual situation. In case of a disagreement between the Bank and the Vendor regarding appointment of an escrow agent, the Bank shall appoint an escrow agent in its entire discretion which shall be final and binding on the Vendor. The Bank and the Vendor shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Vendor.

As a part of the escrow arrangement, the final selected Vendor is also expected to provide detailed code documentation. Any update or upgrade to source code should be informed and brought under escrow or made available to the bank. The execution of Escrow Agreement should be completed within 3 Months from the date of Go Live.

15.3. Compliance with Laws:

Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.

15.4 Compliance in obtaining approvals/permissions/licenses:

Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project.

15.5 Right to Alter:

Right to alter/ delete Components and Quantities specified in the RFP The Bank reserves the right to alter / delete the requirements (Components) specified in the Tender document. The Bank also reserves the right to alter / add the quantity from the quantity specified in the Tender.

15.5 Conflict of Interest:

Conflict of Interest Bank requires that bidder provide professional, objective, and impartial advice and always hold Bank's interest paramount, strictly avoid conflicts with other Assignment(s)/ Job(s) or their own corporate interests and act without any expectations/ consideration for award of any future assignment(s) from Bank. Bidder have an obligation to disclose any situation of actual or potential conflict in assignment/job, activities and relationships that impacts their capacity to serve the best interest of Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if Bank comes to know about any such situation at any time, it may lead to the disqualification of the Bidder during bidding process or the termination of its Contract during execution of assignment.

15.6 Information Ownership:

All information transmitted by successful Bidder belongs to the Bank. The Bidder does not acquire implicit access rights to the information or rights to redistribute the information unless and until written approval sought in this regard. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately, which is proved to have caused due to reasons solely attributable to bidder. Any information considered sensitive by the Bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The Bank's decision will be final if any unauthorized disclosure have encountered. Types of sensitive information that will be found on Bank system's which the Bidder plans to support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc. The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any of the Bank location. The Bidder will have to also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

15.7 Liquidated damages:

The successful bidder must strictly adhere to the schedules for completing the assignments. Failure to meet these Implementation schedule, unless it is due to reasons entirely attributable to the bank, may constitute a material breach of the successful bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this RFP) due to the successful bidder's inability to meet the established delivery dates, and the bank may take suitable penal actions as deemed fit.

Penalty: The successful bidder shall agree to the penalties structure in accordance with the following:

The Liquidated Damages (LD) shall be 1 % of amount for services or goods which have been delayed for each week or part thereof for delay until actual delivery or performance. However, the total amount of Liquidated Damages deducted will be pegged at 10% of the Total contract value (TCV). Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

In this context Bank may exercise both the rights simultaneously or severally. In case the Bank exercises its right to invoke the Bank guarantee and not to terminate the contract, the Bank may instruct to concerned bidder to submit fresh Bank guarantee for the same amount in this regard.

In case delay is attributable to Bank, proper evidence should be produced by Bidder.

15.8 Land Border Sharing Clause:

- 1) The Bidder must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 Order (Public Procurement No. 1), Order (Public Procurement No. 2) dated 23.07.2020 and Order (Public Procurement No. 3) dated 24.07.2020. Bidder should submit the undertaking in Annexure-13 in this regard and provide copy of registration certificate issued by competent authority wherever applicable.
- 2) Para 1 of Order (Public Procurement No. 1) dated 23-7-2020 and other relevant provisions are as follows:
- 3) Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with Competent Authority.
- 4) "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidder stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.
- 5) "Bidder from a country which shares a land border with India" for the purpose of this Order means: -
 1. An entity incorporated, established, or registered in such a country; or
 2. A subsidiary of an entity incorporated, established or registered in such a country; or

3. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 4. An entity whose beneficial owner is situated in such a country; or
 5. An Indian (or other) agent of such an entity; or
 6. A natural person who is a citizen of such a country; or
 7. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.
- 6) The beneficial owner for the purpose of (iii) above will be as under.

In case of a company or limited liability partnership, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more judicial person, has a controlling ownership interest or who exercises control through other means.

Explanation

1. "Controlling ownership interests" means ownership of or entitlement to more than twenty-five per-cent of shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.
3. In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
4. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.
5. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
6. In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
7. An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

15.9 Monitoring & Audit:

Compliance with security best practices may be monitored by periodic computer security audits / Information Security Audits/Statutory and Regulatory audit performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the

Bank. These audits may include, but are not limited to, a review of:

- 1) Access and authorization procedures
- 2) Source code review
- 3) Backup and recovery procedures
- 4) Network security controls
- 5) Program change controls
- 6) The successful bidder must provide the Bank access to various monitoring and performance measurement systems. The successful bidder must remedy all discrepancies observed by the auditors at no additional cost to the bank. For service level measurement, as defined in SLA, data recording is to be captured by the industry standard tools implemented by the Successful bidder. These tools should be a part of the proposed solution.

15.10 Bid Submission:

All responses received after the due date/time be considered late and would be liable to be rejected. GeM portal will not allow lodgment of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any Respondent who lodges a late RFP response for any reason whatsoever, including RFP responses taken to be late only because of another condition while responding.

The details of the transaction viz. scanned copy of the receipt of making transaction are required to be uploaded on GeM website at the time of "final online bid submission The RFP response without proof of amount paid towards Application Money / Bid Security (Annexure 10) are liable to be rejected.

15.11 Integrity Pact:

- 1) Each Participating bidder/s shall submit Integrity Pact as per attached Annexure- 7 duly stamped for ₹500. Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process.
- 2) Bank has appointed Independent External Monitor (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:
 1. Shri Anant Kumar [mail: anant_in@yahoo.com]
 2. Shri Nirmal Anand Joseph Deva [mail: meghanadeva2022@gmail.com]
- 3) For any clarifications/issues, bidders are requested to contact with Bank's personnel in the below mail-id before contacting with IEM.

agmitneo@centralbank.bank.in
cmneoliab@centralbank.bank.in

cmneoliab1@centralbank.bank.in

- 4) IEM's task shall be to review – independently and objectively, whether and to what extent the parties comply with the obligations under this pact.
- 5) IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently.
- 6) Both the parties accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

15.12 Commercial Offers:

- 1) Commercial Bids of only technically qualified Bidders shall be opened based on technical proposal.
- 2) The Commercial Offer (CO) should be complete in all respect. It should contain only the price information as per Annexure-28.
- 3) The commercial offer should be in compliance with technical configuration / specifications as per the scope of the RFP.
- 4) The price to be quoted for all individual items and it should be unit price in Indian rupees.
- 5) In case there is a variation between numbers and words, the value mentioned in words would be considered. The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the commercial Bid inclusive of all costs, taxes and GST. The Bank will not pay any other taxes, cost or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, GST, which shall be paid on actual basis on production of bills with GSTIN. The entire benefits/ advantages, arising out of fall in prices, taxes, duties or any other reason, must be passed on to Bank. The price quoted by the Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out-of-pocket expense. The Selected Bidder will be entirely responsible for license fee, road permits, NMMC cess, LBT, Octroi, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning. Payment of Octroi, entry-tax, etc., alone, if applicable, will be made at actuals, on production of suitable evidence of payment by the Bidder.
- 6) The price is exclusive of taxes like Goods and Services Tax, which shall be paid as per actuals.
- 7) The Manpower / Resource payment should be in accordance with minimum wages act and its subsequent amendments.

During Technical Evaluation the score of the Bidders will not be shared.

Technical offers will be evaluated based on compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders

who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.

In case, any of the successful bidder is unable to honor in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful bidder(s) equally or in any ratio decided by the Bank.

Bank reserves the right to reject any bid offer without assigning any reason or notice and on the sole satisfaction of the Bank, mainly in the following circumstances,

- 1) If the bid offer is incomplete and / or not accompanied by all stipulated documents.
- 2) If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.
- 3) If there is a deviation in respect to the technical specifications of solution offered.

The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons.

Other Terms:

1. No open-source software component including community edition without Enterprise License and OEM's Support will be accepted in the solution.
2. In case bidder quotes open-source software for any requirement given in the RFP, then it is mandatory for the bidder to quote rightful subscription and support charges to ensure compliance with the service levels defined in the RFP.
3. Bank reserves the right to purchase up to 25% additional licenses of the offered platform and its components at the proportionate rates quoted in the Commercial Bill of Material.
4. Bank reserves the right to extend the AMC, ATS, Subscription and FMS of the proposed DKYC & VKYC platform and solution for 2 more years i.e. 6th and 7th year on the same terms and conditions wherein enhancements quoted for 4th and 5th year would be taken as the price reference for the extension.
5. The bidder should provide the cost for every line item which has been mentioned in the Bill of Material (BOM).
6. Bank reserves the right to implement or drop any of the listed items without assigning any reason. If the cost for any line item is indicated as zero, then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
7. The price quoted for the project should be an all-inclusive price including any taxes, expenses, levies, GST and is a fixed price.
8. Bank will deduct applicable TDS, if any, as per the law of the land.
9. The quoted fixed cost against each item shall remain unchanged till the completion of the Project(s).
10. The base project location will be Mumbai/Navi Mumbai/Hyderabad.
11. The TCO in words is amount on which the commercial evaluation will be conducted.
12. All prices should be valid for a period of 5 years from the date of contract execution / signing.

13. Bidder should factor all the expenses like travelling, boarding, lodging etc. for the resources involved in the contract. No other expenses will be paid by the Bank apart from amount specified in Commercial Bid.
14. Bidder shall depute resources on-site of the project implementation location(s) for carrying out the task as specified in this document.
15. The cost quoted is in fixed price and no increase in rate will be admissible by the Bank for whatsoever reasons during the contract period.
16. The cost quoted also includes the cost of deliverables for all the phases of the Project.
17. Further, bidder should abide by all the terms and conditions mentioned in the Request for Proposal document.
18. Fee is payable only on actual availing of services and no minimum or fixed fees are payable.
19. Per Person-day rates applicable in case of enhancement of scope in future shall be as per the rate for the respective year quoted in the Commercial Bill of Material. The amount shall be paid on pro-rata basis based on the actual usage. Any unused person-days shall be carry forwarded to the next year.
20. The ATS cost System Software shall be minimum 15% of Product Cost.

15.13 Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and any revision thereto will be applicable for this RFP. As the evaluation of successful bidder is on basis of "Technical Competence and the Price Quoted", the margin of purchase preference to Class-I local supplier shall not be applicable under this RFP.

15.14 Payment Terms

Payment will be released by the Central Office of Bank from where the purchase order is issued. All the Payment shall be made in Indian Rupees only.

The payments will be released only on completion of respective milestones/schedules and sign-offs by Bank Team towards Product, License, Subscription, Implementation, AMC, ATS, FMS and any other Cost as under.

A) Application License Cost: These terms are applicable for each of the two platforms i.e. DKYC & VKYC.

Project Milestones	Percentage of License Cost which will be paid
Delivery of perpetual enterprise Licenses and Installation of Application Software in UAT, DC & DR. (after due inspection and acceptance at DC & DRC)	40%
Successful completion of the customization, UAT sign and go live of 10 journeys as per Bank's requirements. This milestone shall be considered as project Go Live date.	20%
Successful completion of the customization, UAT sign and go live of another 10 journeys as per Bank's requirements	20%
3 Months from the date of Go Live or DR Drill completion whichever is earlier and on execution of Escrow agreement	20%
Total	100%

B) Third Party Software License Cost

Project Milestones	Percentage of License Cost which will be paid
Delivery of Licenses on Bank's name and Installation of the software on Bank's UAT, DC & DRC. The amount shall be released on submission of the proof of payment and proof of Licenses in the name of the Bank which should also mention the period of validity.	100%

Annual subscription of Licenses	
The amount shall be released on submission of the proof of payment and proof of Licenses in the name of the Bank which should also mention the period of validity.	100%

C) Implementation Cost

The table mentioned below is applicable to each of the 30 journeys mentioned in Table-2 of Scope. The implementation cost is payable per journey against the following four milestones mentioned below.

Project Milestones - Implementation, System Integration and Migration	Percentage of Implementation Cost which will be paid
Successful completion of current state assessment, gap analysis and systems requirement specifications (SRS) / Business Requirement Document Sign off by Bank	20%
Successful completion of the customization and UAT sign off	40%
Go Live of Journey	30%
3 Months from the date of Go Live or DR Drill completion whichever is earlier	10%
Total	100%

D) Other Costs

D	Training Cost	100% will be paid after training is completed
E	ATS Cost	ATS of DKYC & VKYC application will be paid quarterly in arrears. For ATS of third-party software, the amount shall be released on submission of the proof of payment and proof of Licenses in the name of the Bank which should also mention the period of validity.
F	Facility Management Cost	Quarterly in arrears basis, at the end of each quarter, on actuals, as per the bill submitted by the Bidder and on verification of the attendance of the resources by Bank.
G	User Defined Customization (Change Requests done by the Offshore Team)	50% after the UAT Sign off by the Bank
		50% on Go-Live

The claim of payment should contain proof of delivery, installation note and User Acceptance Report signed with date by an authorized official of Central Bank of India at the respective sites, waybill etc. All the payments will be released after realizing penalty charges/LD for late

delivery, if any.

15.15 Terms & Conditions:

Warranty & AMC

Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of five years from the Go-Live of project.

For in-scope software licenses, warranty period should be of 5 years from the date of installation or 61 months from the date of delivery whichever is earlier. The comprehensive onsite warranty shall be with OEM back-to-back support. The word "warranty" in this document refers to "comprehensive onsite warranty". Bidder must factor the costs in the Bill of Material accordingly. As part of warranty, the Bidder must:

- i. Provide on-site comprehensive support for software components as well as OS & DB provided as part of this RFP
- ii. Have back-to-back arrangements with respective OEMs for the maintenance services
- iii. Warrant all software against defects arising out of faulty design, materials and media workmanship etc., for a period of five years from the date of acceptance & Go-Live of the application.
- iv. Agree that Bank will not be liable to pay any additional amounts in respect of any sort of maintenance covered under the scope of this tender during the tenure of the contract. Free on-site maintenance services shall be provided by Bidder during the period of contract. Change Order to comply any statutory / Regulatory / Government requirement will be undertaken by bidder without any cost to Bank during the contract period of 5 years and the extended period of contract if any.
- v. In case Bank desires to get the services delivered by their appointed Bidder or System Integrator, then the OEM shall transfer such services to that preferred Bidder at no additional cost to Bank
- vi. In case of any issue with related software supplied by Bidder, Bank or its appointed System Integrator shall log a call with Bidder (who has supplied the software). It is responsibility of Bidder to resolve the issue with the assistance of the OEM, if deemed necessary. Bank or its appointed System Integrator shall promptly notify Bidder in writing/e-mail/fax of any claims arising under the maintenance services
- vii. Provide all future software upgrades and patches for all components of the solution and assist Bank or its System Integrator to install the same, if Bank desires during period of warranty free of cost

Cost & Currency Price Composition

The Bidder should quote unit price in Indian Rupees (without decimal places) for all components (software etc.) and services on a fixed price basis, as per the commercial Bid inclusive of all costs and GST. Bank will not pay any other taxes, cost or charges.

Goods and Services Taxes (GST) and its Compliance

Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Bidder shall have to follow GST Law as per time being enforced along with certain mandatory feature mentioned hereunder:

- (a) TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the Bidder of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person
- (b) It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to Bank by way of commensurate reduction in the prices under the GST Law
- (c) If Bidder as the case may be, is blacklisted in the GST (Goods and Services Tax) portal or rating of a Bidder falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract
- (d) Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Bidder shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

Fixed Price

The commercial offer shall be on a fixed price basis. No price variation relating to increases in dollar price variation etc. is permitted.

- a) No advance payment will be made. TDS and any other taxes on payments will be deducted as applicable.
- b) All the payments will be made to bidder electronically in Indian Rupees only.
- c) Payment shall be released on submission of necessary proof and documents like original Invoices, Warranty Certificates, Performance Bank Guarantee, Signed Service Level Agreement, and Delivery of Software Licenses etc. subject to acceptance by Bank, submission of Letter issued by Bank in respect of completion of User Acceptance Test (UAT), documents as required by Bank like manual & documentation, training etc.
- d) Invoices shall be raised post milestone sign off for services billing.

Generally, Bank will pay invoices within 30 days from the date of receipt of physical invoice by the Bank, except for those portions of any invoice that the Bank disputes in good faith and in writing. No penalty /Interest will be paid for the delayed payment.

15.16 Intellectual Property

15.16.1 The Bank intends to procure and own the DKYC & VKYC Solution developed by the successful bidder

15.16.2 The successful bidder should provide comprehensive warranty for the application and Bank will be paying the AMC if required thereafter completing the warranty period

- 15.16.3 The Bank should have the ownership of all the Intellectual Property rights associated with the concept, design and flow both future and present, even after the warranty/AMC period.
- 15.16.4 While the Bidder shall retain the intellectual property rights for the Platform, it is required that bidder shall grant the perpetual License to the bank for the bank's exclusive use without limitation on the number of users. The Bidder shall place the source code of customizations done for the bank (and the procedures necessary to build the source code into executable form) for the application software, in Independent escrow with a reputable agency (a bank or established software escrow firm in India) acceptable to the Bank during the contract period. The Bidder shall provide the source code of customizations done for the bank for the unlimited and unrestricted use by the Bank. Bank shall have the rights to modify the platform and source code without any restrictions. Bidder warrants that the Software provided shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.
- 15.16.5 Source code for customization done for Bank in DKYC & VKYC solution and for other related services shall be provided by the bidder to the Bank for unlimited and unrestricted use by the Bank.
- 15.16.6 Bidder shall also provide all related material but not limited to flow charts, annotations, design documents schema, development, maintenance and operational tools and all related documentation
- 15.16.7 The Bank should have the rights to modify the platform and source code without any restrictions
- 15.16.8 In case the successful bidder is coming with software which is not its proprietary software, then the bidder must submit evidence in the form of agreement it has entered with the software vendor which includes support from the software vendor for the proposed software for the full period required by the Bank

15.17 Enterprise Licensing

1. The Platform should follow enterprise-wide perpetual licenses for all modules offered without any constraint like number of users, transactions, APIs, screens, delivery channels, devices, branches etc.
2. License for the DKYC & VKYC Solution should cover all installations like primary site, DR, other environments like Development, UAT, Sandbox etc. based on Bank's requirements without limitations on number of users, transactions, servers, usage, integrations etc.
3. All software envisaged is required to be on-premises software licensed to Bank
4. The successful bidder must:
 - I. Provide licensing policy to the Bank covering the platform, solution, hardware, software, or any other component supplied as part of this RFP.

- II. Ensure the software supplied must be the latest version of the software supplied by the OEM. Beta versions of any software shall not be accepted.
 - III. Consider the disaster recovery environment while proposing the software licenses
 - IV. Offer technical and functional support of the service for contract tenure post implementation of solution.
 - V. Provide complete functional and technical solution for any new platform, model, and OS and DB upgrade within thirty days of launch in India without any extra cost.
 - VI. Ensure DKYC & VKYC Platform along with final customization should be VAPT certified at no extra cost to Bank.
 - VII. Ensure support contract for the solution should include any and all statutory and regulatory (RBI, NABARD, NPCI, IBA, IRDAI etc.) global or country wide or state- wide updates, cyber security framework updates etc. free of cost during the tenure of contract.
5. Ensure support contract for the solution should include program updates, patches, fixes, and critical security alerts as required.

15.18 Facility Management and Maintenance Services

1. Bidder shall designate one of its personnel as the Project Manager, to interact with the Designated Customer Support Contact from the Bank for the purposes of getting approvals, progress report, discussing and resolving issues, arranging meetings, successful implementation of this project etc. Bidder should also provide Facility Management having hierarchical and scope based support personal such as L2 and Team leads.
2. During the implementation phase the complete development team shall be stationed at Bank's office at Mumbai / Navi Mumbai. Bidder should factor such costs in the commercials. Post go live of the platform, the development team may be moved back from Bank's office.
3. During implementation phase there should be a team of at least 10 resources L3 – 3 and L2 – 7 including resources of OEM.
4. For FM services there should be a team of 5 resources (L2 - 5) including One DBA. However, Bank shall decide the actual requirement of the resources after due assessment.
5. There should be a team of L3 & L2 resources preferable self-sufficient Agile team to attend bug fixes, handle Change Requests, maintenance and support.
6. Bidders should ensure to manage and maintain software as mentioned in the RFP and as per the agreement the bidder should deploy at Bank's Site required number of onsite technical experts throughout contract period. The deployed resources (to have adequate skill, good academics & be technically sound) should manage the above-mentioned scope of work and have experience for monitoring & management of the proposed solution. The deployed resources should be available on all working days of the Bank. The bidder should be able to recruit/ deploy the resources within 30 days of placing the order/LOI for the onsite technical resource.
7. Bidders to ensure that deployed resources should be competent to develop/ configure/

handle/ integrate/ maintain/ manage/ Implement/ Test / Go-live the proposed DKYC & VKYC solution.

8. Bidder should ensure that the onsite resources should perform testing, support, monitoring, implementation, integration, Trouble Shooting, reporting, RCA reports, coordination with bank's teams, Audit compliance, any other statutory compliance, Patch Installation (OS, DB, App and Software) fixes, analytics, fraud risk/rule management & monitoring, day to day MIS reports, Regulatory reports, conducting DR Drill, backup/restore. These activities are an indicative gist of activities which may increase depending upon the requirement of the DKYC & VKYC Ecosystem.
9. Bidder should ensure continuity of resources during the implementation phase.
10. The Onsite resources shall also prepare and maintain the detailed process documentation, Standard operating procedure and other documentation as required for implementation, maintenance and management of the solution and same shall be submitted before signoff and within 30 days of GO-LIVE of solution & be properly updated during the contract period.
11. The deployed resources shall be on the bidders' payroll/contracts and will not be having any employment right with the bank. These resources will not have any right whatsoever to lodge claim of any nature directly or indirectly with the bank. The selected bidder shall address such issues without involving the bank. The onsite resources provided for Facility Management at Bank's premises should be on payroll of the successful bidder and not on any third party payroll. In case, if the successful bidder must depute third party resource payroll and not bidder's payroll, the permission of the same is to be taken from the Bank before deployment and it will be successful bidder's responsibility for any action taken on part of the deployed resource by the bidder.
12. The deputed persons must maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised/ disclosed/ misused/ misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to fully compensate the bank of loss incurred by the bank. Bidder is expected to adhere to Bank's request for removal of any personnel, if bank notices any negligence/gross misconduct/violation of trade secret/disclosure of bank's data to third party and any decision of the bank in this regard would be final and binding upon the selected vendor.
13. Bidders to ensure that the resources deployed for onsite support should possess minimum 2-year experience. Bank reserves the right to claim change in resource based on the performance of the resources.
14. If Bank must increase or decrease resources at onsite or off-site same shall be done at the same rate as provided in this RFP.
15. Monitoring and Management of DKYC & VKYC solution including infrastructure deployed. Bidder should provide the dashboard for Real-time monitoring of DKYC & VKYC traffic/transactions/API calls etc. and get the transaction status and its reason of

failure, if any. Breakup of Business and Technical decline. The dashboard should also have the capability to generate reports like count of Financial & No-Financial Transactions for a period, Number of Customers on-boarded etc.

16. Configuration management: The successful bidder must ensure that all supplied & installed infrastructure & solutions are updated with the latest configuration and both the sites (DC & DR) have consistent configuration.
17. Patch Management: The successful bidder must ensure that all supplied & installed infrastructure & solutions are updated with patches as and when they are released after due testing. Critical patches should be applied immediately as per Bank Policy.
18. Service Level Management, Service reporting- Maintain the service levels as per the RFP and provide a periodic report to the Bank assessing all device performance under the scope of RFP against the Service Levels. Service Levels will include Availability measurements and Performance parameters (Utilization of CPU, RAM, storage, TPS, performance etc.)
19. Change Management: The successful bidder must ensure that all supplied & installed infrastructure & solutions related changes are properly updated and recorded with version controlling/rollback and to have consistent setup both the sites (DC & DR).
20. Coordination with different Bank's partners and other regulatory entities. Work as per Standard Operating Processes defined by the Bank, create and maintain SOPs as per project requirement.
21. Co-ordinate with Bank's IT Team or teams identified by the Bank. Preliminary trouble shooting of any issue related to the DKYC & VKYC service/ platform as reported by Bank staff or customer.
22. Update ticket status in Bank's monitoring tool or in such a manner that same will readily available as & when required with logging.
23. Log ticket bidder internal helpdesk for solution related issues through any of the following mode: Telephonic, Email, Ticketing Tool etc.
24. Maintain log of all down calls for MIS purpose and provide daily, weekly, monthly, quarterly reports to Bank in formats finalized during operations.
25. Interface with and coordinate problem identification and resolution with the appropriate support organizations within or external to the Bank; Co-ordinate with OEM for ticketing, escalation and resolution of issues and restoration of hardware or associated software.
26. Provide a periodic report to the Bank assessing all device performance under the scope of RFP against the Service Levels.
27. Operation Management: The successful bidder should review the performance of the equipment/ technology deployed with the bank on a bi-annual basis and take necessary upgrades, i.e. of equipment and software, as and when required without any additional cost to the Bank. Successful bidder should monitor measures, evaluates, and records status and

performance information about all the equipment and software brought in by the bidder to aid in performance monitoring and tuning of the environment. Performance metrics should include utilization, throughput and other critical system needs. The successful bidder shall implement proactive procedures to address trends identified from performance and monitoring data. The successful bidder should provide standard reports that are to be provided to designated Bank personnel.

28. Successful bidder should fix any security findings/vulnerabilities identified by various security agencies hired/consulted by the Bank without any additional cost during the contract period. Further, if the security observation(s) cannot be closed by applying updates/patches/fixes/upgrades to the supplied equipment and replacement is the only option to close the observation(s), then the successful bidder must replace the device(s) with device meeting all the specifications of the RFP at no extra cost to the Bank. However, the Bank reserves the right to waive off the hardware replacement depending on the type of vulnerability and its associated risk.
29. End of Sales / End of support: The Bidder must ensure that any solution/equipment supplied as part of this RFP should not have either reached or announced 'End of Sales' (1 years from last date of submission of Bid.) or end of support for at least 5 years from the date of go live. In the event if any equipment supplied by the bidder reaches end of support, within the 5 years period from the date of supply, the bidder must replace the equipment with devices having equivalent or upgraded specification, at no additional cost to the Bank or revamp the entire solution (if required).
30. The Solution including Application & Hardware shall have a roadmap for 5 years from the Go Live date. A certificate to this effect had been provided by the bidder and in Annexure-24. Continuing the services / maintenance beyond 5 years would be as per the Service Continuity clause in this RFP.
31. Facility Management (FM) on all working days of the bank shall be a part of solution for entire contract period. End to end service support shall be provided by the bidder. The bidder shall ensure the availability of dedicated FM personnel on all working days of the bank during the contract period. The bidder shall ensure that the FM personnel are available exclusively for DKYC & VKYC. FM personnel shall have a graduate degree at a minimum, have 2 years of experience in the field of DKYC & VKYC support and have in-depth knowledge of the solution provided. Bank reserves the right to interview the FM personnel including Project Director intended to be deployed and if not found suitable may reject them.
32. The bidder shall provide mission critical support for the software for DKYC & VKYC solution. The mission critical support includes support with site engineers for software on all working days of the bank.
33. The bidder shall deploy a Project Manager having minimum 10 years of work experience in the same field stationed at Mumbai / Navi Mumbai for entire contract period.
34. Incident Management -

The bidder shall establish robust Incident Management process including:

- a) Provide 24 x 7 support for incident management for all components of the DKYC & VKYC
- b) Provide automated fault detection and resolution
- c) System to do automatic dispatching to avoid delays and automated messages to field engineers
- d) System to provide for automatic escalation in case of problem not getting resolved
- e) Do proactive maintenance of all devices
- f) Carry out remote resolution before actual dispatch, if necessary
- g) Analyze machine performance and suggest improvement

35. Service desk

- a) Providing technical assistance for logging, troubleshooting and managing the service requests for the DKYC & VKYC
- b) Monitoring, alerting, troubleshooting and resolution of incidents/ problems for the DKYC & VKYC solution
- c) Monitoring and alerting on the health of the DKYC & VKYC
- d) Providing technical assistance for logging, troubleshooting and managing DKYC & VKYC related service requests

36. Accounting and Reconciliation

- a) Recording and Storage of all transactions pertaining to the DKYC & VKYC and associated services, as described in the Bank
- b) MIS reports for all DKYC & VKYC and associated activities on a routine basis or as requested by the Bank
- c) Ability to interface with the Bank's data and analytics systems to provide the reports required by the Bank, in the format as prescribed by the Bank

37. Information protection

- a) Backup, storage and restoration of data related to the DKYC & VKYC and associated services, in a secure and reliable manner
- b) Backup, storage and restoration of configuration data for the DKYC & VKYC and associated infrastructure
- c) Backup, storage and restoration of any mission critical data related to the DKYC & VKYC and associated services

- d) Backup, storage and restoration to enable the Bank to achieve regulatory compliance as per Bank, RBI or other applicable guidelines.

38. Fraud detection and protection

- a) The Fraud Management System should be configurable, customizable, highly scalable and provide real time fraud monitoring
- b) The solution should have support for future integration with AI/ML-based modules (e.g., advanced fraud detection, customer segmentation).
- c) The system shall have rules to provide basic functionalities to monitor the fraud and risk aspects.
- d) Block DKYC & VKYC use by country and/or predetermined MCC (Merchant Category Codes) codes

39. Business Continuity/ Disaster Recovery

- a) Implementing and maintaining BCP and the DR readiness (including data replication), for the DKYC & VKYC and associated services to meet the Bank's RTO and RPO Objective.
- b) Replication of data between the primary and the DR site from the disaster recovery perspective.
- c) Bidder to perform Drill (Switch-over and Switch-back) activity as and when scheduled by the Bank

40. Compliance and assurance

- a) Assisting the Bank in attaining and ensuring on- going compliance to various regulatory and data security/ privacy requirements
- b) Addressing relevant threats/ risks identified in a proactive manner and through audit observations
- c) Providing analysis and MIS for Switch and associated services related data, to demonstrate audit readiness and adherence to the agreed service levels.
- d) For all existing applications, BIDDER shall submit Data Dictionary (wherever feasible) as a part of System documentations.
- e) Shall submit within 10 days from signing of this Agreement, an Application Integrity Statement from application system vendor providing reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs and free of any covert channels in the code
- f) Compliance to Bank IS policy and other related policy, adherence to Bank Minimum Baseline security requirement , adherence to all internal and external audits and

Quarterly/half yearly VAPT requirement

- g) Bidder should close the audit and VAPT observations within the stipulated timeline
- 41. Provide preventive and breakdown maintenance activities without any impact on day-to-day operations to maintain the required business uptime covering 24*7*52 weeks
- 42. Provide 36 hours' notice to the Bank and seek approval before executing any preventive maintenance
 - a) This notice should have details of the changes being implemented including testing results, impact to DKYC & VKYC 's users, communication process for users, fallback process and any other documentation requested by the Bank
 - b) Provide updates throughout the maintenance window at frequency agreed with the Bank
- 43. Provide status of support activities and tickets on a regular basis to the Bank and attend all required meetings on governance of the IT systems
- 44. Ensure root cause analysis and ticket management processes are followed as per SLA timelines defined by the Bank in this RFP

15.19 Mandatory Training/Knowledge Transfer

15.19.1 The successful bidder is responsible for imparting required training to the Bank's project and core teams and support vendor (if any) to configure, use and maintain the DKYC & VKYC Platform

15.19.2 The successful bidder shall organize following training to the Bank's team:

15.19.3 Five working days training to the Bank's Core Team (including support vendor, if any) to be imparted before UAT in multiple batches based on agreement with the Bank

15.19.4 Comprehensive training to the Bank (including support vendor, if any) once in a year during the contract period, as and when required by the Bank

15.19.4.1 Training to IT team should cover configuration, operations, maintenance & support, administration of software, platform architecture and components, installation, troubleshooting processes, user management, data base administration and maintenance, report generation, security management, backup & disaster recovery etc.

15.19.4.2 Training to business user groups should cover operational features, functionalities in the modules, report generation, auditing, and any other operational activities

15.19.4.3 Training to the Business Operations team to on-board partners, view reports, integrate partners using APIs, or any other activity to be handled by the

concerned team

15.19.5 Training material to be provided to all the trainees (including support vendor, if any) with illustrations of scenarios, required actions, possible support features etc.

15.19.6 All trainings will be conducted onsite at Central Bank office in Mumbai/Navi Mumbai Area.

15.19.7 The successful bidder should indicate the optimum number of days / hours required for all training programs onsite

15.19.8 The successful bidder should provide self-paced training content with video, audio, and subtitles (e-Learning material)

15.20 Service Level Agreement

This section describes the service levels that has been established for the Services offered by Bidder to the Bank. Bidder shall monitor and maintain the stated service levels to provide quality customer service to the Bank. The Service Level Agreement (SLA) with the successful bidder will be part and parcel of the RFP document. Therefore, please note and ensure that all such queries are to be raised before bidding. Any query/ request for review of any clause of RFP/ SLA after the completion of bidding process shall not be entertained on SLA. However, Bank may add clauses depending on the solution finalized at the time of execution of SLA and as per Policy guidelines.

The Vendor understands the largeness of this Project and that it would require tremendous commitment of financial and technical resources for the same, for the tenure of Contract under this RFP. The Vendor therefore agrees and undertakes that an exit resulting due to expiry or termination of Contract under this RFP or for any reason whatsoever would be a slow process over a period of six (6) months, after the completion of the notice period, and only after completion of the Vendors obligations under a reverse transition mechanism. During this period of Reverse Transition, the Vendor shall continue to provide the Deliverables and the Services in accordance with the contract under this RFP and shall maintain the agreed Service levels. The Bank shall make payment for these services as per terms.

The Bank expects that the successful Vendor to adhere to the following minimum Service Levels:

15.20.1 Any fault/ issue/ defect failure intimated by Bank through any mode of communication like call/e-mail etc. are to be acted upon, to adhere to the service levels. Business/ Service Downtime and Deterioration shall be the key considerations for determining "Penalties" that would be levied on the Successful Vendor.

15.20.2 The Vendor should have 24X7X365 days monitoring, escalation and resolution infrastructure.

15.20.3 Time bound problem addressing team (onsite) for the complete contract period.

15.20.4 Vendor to arrange for update required in the system to meet the changes suggested by RBI/ Govt. of India/ regulatory authorities towards compliance as part of ATS at no extra cost to bank for the entire contract period. Any delay in meeting the

timelines would result in penalty.

SLA for DKYC & VKYC :

Vendor should guarantee a minimum uptime of 99.95%, calculated on a monthly basis. Application (As a whole / any module of the application) availability will be 99.95 % on 24x7x365 days. The penalty will be calculated as per the details given below.

Uptime percentage - 100% less Downtime Percentage

Downtime percentage - Unavailable Time divided by Total Available Time, calculated on a monthly basis.

Total Available Time – 24 hrs. per day for seven days a week excluding planned downtime

Unavailable Time - Time involved while the solution is inoperative or operates inconsistently or erratically.

Uptime Percentage	Penalty Details
100% to <= 99.95 %	No Penalty
99.95% to <= 99 %	5% of cost of monthly billing
99 % to <= 98%	7% of cost of monthly billing
98% to <= 97%	10% of cost of monthly billing
Below 97% - Minimum 10% of cost of monthly billing & 1% for every incremental increase in 0.5% downtime	

The payment terms are quarterly in arrears, however, penalty amount will be applied on the monthly amount payable based on SLA breach. If bifurcation of quarterly invoice is not provided, Bank will divide the quarterly billing amount in the uptime percentage and would be calculated on monthly basis and the calculated amount would be adjusted from every subsequent quarter payment. The SLA charges will be subject to an overall cap of 10% of the Project Cost and thereafter, Bank has the discretion to cancel the contract. If Vendor materially fails to meet an uptime of 99.50% for three (3) consecutive months, the Bank may have the right to terminate the contract. In case if there are no pending invoices to be paid by the Bank to the bidder, the bidder has to submit a pay order / cheque payable / credit note at Mumbai in favor of Central Bank of India for the same within 15 days from the notice period from the Bank.

Availability Service Level Default

1. Availability Service Level will be measured on a monthly basis.
2. A Service Level Default will occur when the vendor fails to meet Minimum uptime (99.95 %), as measured on a monthly basis.

Bidder shall determine the severity levels based on the criteria mentioned below:

Severity Level	Number of users impacted	Effective Downtime
Severity 1	Issues which prevent the DKYC & VKYC Platform from being used at all, degrade critical functionalities and no workaround exists, or disrupt performance of the platform for all or majority of users	100%
Severity 2	Issues which cause significant loss of functionality or performance of the DKYC & VKYC Platform, or degrade functionalities for majority of users while a workaround may exist	90%
Severity 3	Issues related to moderate loss of non-critical functionality or performance of the DKYC & VKYC Platform, failure of minor features etc.	80%
Severity 4	Issues related to low impact functionality of the DKYC & VKYC Platform or informational requests	20%

SLA Penalty Calculation:

E.g. - There is an incident which occurs under the Severity Level 2 for which the downtime is for 5 hours in a month. Therefore, the effective downtime for the month would be:

$$5 \text{ hours} \times 90\% = 4.5 \text{ hours}$$

Therefore, the downtime of 4.5 hours would be considered due to this incident while computing the availability of the application.

Bidder is required to provide evidences for ascertaining Severity Levels in absence of which Severity level for the incident would be considered as 1 for the purpose of penalty calculation. Severity level 1 & 2 may attract penalty on both FMS & ATS on case to case basis.

SLA for Onsite Support Facility Management

Bidder will have to guarantee a minimum of 99% per resource availability (i.e. attendance of each of the resources), calculated on a monthly basis.

Resource availability percentage will be calculated as (100% less Person non-attendance Percentage) Person non-attendance percentage will be calculated as (Unavailable Time divided by Total Available Time), calculated on a monthly basis. Total Available Time is 8 hrs. per day per person for a week.

The uptime percentage would be calculated on monthly basis and the calculated amount would be adjusted from every subsequent quarter payment. The yearly SLA charges will be subject to an overall cap of 10% of the Yearly Resource cost and thereafter, the contract may be cancelled. In case if there are no pending invoices to be paid by the Bank to the bidder, the bidder has to submit a pay order / cheque payable / credit note at Mumbai in favor of Central Bank of India for the same within 15 days from the notice period from the Bank.

Availability Service Level Default for Facility Management

Bidder will have to guarantee a minimum attendance of 99 % per resource (i.e. attendance of each of the resources), calculated on a monthly basis. Attendance percentage will be calculated as (100% less Person non-attendance Percentage) Person non-attendance percentage will be calculated as (Unavailable Time divided by Total Available Time), calculated on a monthly basis.

The attendance percentage would be calculated on monthly basis and the calculated amount would be adjusted from every subsequent quarter payment. The yearly SLA charges will be subject to an overall cap of 10% of the Yearly Resource cost and thereafter, the contract may be cancelled. In case if there are no pending invoices to be paid by the Bank to the bidder, the bidder has to submit a pay order / cheque payable at Navi Mumbai in favor of Central Bank of India for the same within 15 days from the notice period from the Bank.

1. Availability Service Level will be measured on a monthly basis.
2. A Service Level Default will occur when the Service Provider fails to meet Minimum uptime (99%), as measured on a monthly basis.

In case any resource is not available continuously for more than 4 hours a day (Under normal circumstances) Or 1 day in case of unplanned / emergency leave of any resource then the Bidder should immediately provide the Bank with an equivalent standby resource for that resource.

If Bidder fails to meet the uptime guarantee in any month then the Bidder will have to pay the following compensation adjusted with every subsequent quarter payment:

$(\text{Minimum attendance Percentage} - \text{attendance Percentage}) \times \text{Current Years Monthly Contract value}$

Service Levels during implementation phase

1. The Bidder is expected to complete the responsibilities that have been assigned as per the implementation timelines mentioned in Section - Project timelines.

Penalty would be levied for delivery, installation, and implementation delays for DKYC & VKYC Platform and shall be a maximum of 10% of the total cost of that solution from the finalized bidder for the bank. The bidder is required to adhere to the Service Level

Agreements as mentioned below for the operations phase.

After acceptance of respective solutions by the Bank:

System Availability

System availability is defined as $\frac{\{(Scheduled\ operation\ time - system\ downtime)\}}{(scheduled\ operation\ time)} * 100\%$.

Where:

1. Scheduled operation time means the scheduled operating hours of the System for the month. All planned downtime on the system would be deducted from the total operation time for the month to give the scheduled operation time.
2. System downtime subject to the SLA, means accumulated time during which the System is not available to the Bank's users or customers due to in-scope system or infrastructure failure, and measured from the time the Bank and / or its customers log a call with the Bidder's help desk of the failure or the failure is known to Bidder from the availability measurement tools to the time when the System is returned to proper operation.
3. Critical and Key infrastructure of Data Centre, Disaster Recovery Centre and Near Site will be supported on 24x7x365 days basis.
4. Downtime shall commence when the respective hardware and or its associated software fails.
5. Uptime will be computed based on service availability of the in-scope components. Also, non-compliance with performance parameters for business and system / service degradation will be considered for downtime calculation.
6. Response may be telephonic or onsite. In case the issue cannot be resolved telephonically, Bidder (as per the criticality and nature of the issue) will provide onsite assistance at respective locations (DC, DRC and Near Site) within response resolution window.
7. If any one or more of the components defined in —Critical at the Data Centre, Disaster Recovery Facility and Near Site are down resulting in non-availability of Solution, then affected services / components listed in the —Critical availability measurements table shall be considered for calculating the system downtime.
8. The Data Replication between the DC and Near Site should be storage to storage based Oracle Log replication and adopted technique for DC and DRC is currently on Oracle Data Guard based replication.
9. Service Levels will be complied with irrespective of the customizations that would undergo during the tenure of the Contract.
10. Typical Resolution time will be applicable if services are not available to the Bank's users and customers and there is a denial of agreed services.
11. The bidder to provide warranty & AMC support on all days (24X7X365 days) for period of contract
12. Bank has defined in-scope services and corresponding SLAs as under, Bank shall evaluate the performance of the Bidder on these SLAs compliance as per the periodicity defined.
13. The Successful Bidder shall provide, reports to verify the Successful Bidder's performance and compliance with the SLAs. Automated data capturing and reporting mechanism will be used for SLA reporting. The bank will leverage existing/future EMS tools to monitor and manage the Solution/IT Infrastructure.

14. If the level of performance of Successful Bidder for a particular metric fails to meet the minimum service level for that metric, it will be considered as a Service Level Default.
15. Overall cap for penalties over the tenure of the contract will be 10% (ten percent) of the contract value.
16. Penalties if any, as defined by SLAs, shall be adjusted in the payment of a quarter. Balance penalties, if any shall be levied in the payment for the subsequent quarter.
17. The Bidder should provide Support contract backline to OEM for the complete duration of contract period. Letter to be provided by OEM for the backline proof, prior to release of payment.
18. Bidder agrees to ensure that all the items / products used for delivering services to the Bank including all components are new and are using state of the art technology. Bidder shall provide such proof of the new equipment (e.g. Copy of invoice etc.) to the Bank. In case of software supplied with the system, Successful Bidder shall ensure that the same is licensed and legally obtained in the name of end customer i.e., Bank with valid documentation made available to the Bank.

Note: All service level penalties will be reconciled at the end of every quarter.

Service Level Default

Service Levels will be measured on a monthly basis. The Bidder's performance to Service Levels will be assessed against Minimum Expected Service Level requirements for each criterion mentioned in the Availability measurement table.

An Availability Service Level Default will occur when:

The Bidder fails to meet Minimum Service Levels, as measured on a monthly basis, for a particular Service Level.

- 1) Service Levels will include Availability measurements and Performance parameters.
- 2) Bidder will provide Availability Report on monthly basis and a review shall be conducted based on this report. A monthly report shall be provided to the Bank at the end of every month containing the summary of all incidents reported and associated Bidder performance measurement for that period. The reports submitted to Bank may verified with existing EMS tools for measuring the performance.
- 3) Performance measurements would be accessed through reports, as appropriate to be provided by Bidder e.g. utilization reports, response time measurements reports, etc.
- 4) Cost Reference that is mentioned is billing value for the defaulted period & defaulted component for which SLA will be calculated.

Liquidated damages for SLA Default

The Bank will consider the inability of the bidder to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the bidder. The liquidation damages represent an estimate of the loss or

damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, Operationalization, implementation, training, acceptance, warranty, maintenance etc. of the entire scope of the tender) by the bidder.

Installation will be treated as incomplete in one/all of the following situations:

Non-delivery of any component or other services mentioned in the order Non-delivery of supporting documentation.

If the bidder fails to deliver any or all of the Goods or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% of the of the order value of the product and or services cost per week or part thereof until actual delivery or performance, (above 3 days will be treated as a week); and the maximum deduction is 10% of the contract value. Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

In case of temporary substitute equipment installation, the temporary substitute equipment should be replaced by the original equipment duly repaired or replaced with similar equipment of same capacity or higher capacity, failing which a penalty of 0.5% per day of the item cost will be imposed for the number of days the device is down subject to a maximum of 10% of the equipment cost.

The amount of penalty will be recovered from the successful bidder from payments due to them. In case, no payments are due, the successful bidder has to remit the same within 15 days of claim from the Bank failing which the Bank shall be at liberty to invoke Bank Guarantees provided for during warranty period by the successful bidder. However, if the DKYC & VKYC Platform application is down due to the reasons attributable to the Bank, the successful bidder has to submit proof for the same for not levying the penalty.

Availability Service Credit Computation

In the event of an Availability Service Level Default, the Bidder shall pay the Bank an Availability Service Credit that will be computed in accordance with the following formula:

Monthly Service Level Default = Minimum Service Level – Monthly Actual Service Level

Availability Service Credit = Quarterly Service level default X (Summation of Cost

References)

In the event that an Availability Service Level Default has occurred for more than one service level requirement, the sum of the corresponding Availability Service Credits shall be credited to the Bank. Bidder shall review with the Bank, on a monthly basis from the start of Contract Execution, any entitlement of the Bank to an Availability Service Credit.

The total amount of Availability Service Credit that Bidder is obligated to pay the Bank shall be reflected on the invoice provided to the Bank in the quarter after the quarter in which the Service Levels were assessed. The Bank shall be entitled to deduct the Availability Service Credit amount from the amounts payable by the Bank to the Bidder as per the invoice,

respective credit note against those invoices needs to be provided by Bidder.

Example 1

Assume for a particular service level requirement (e.g.: Availability of Key Business Infrastructure Elements), the minimum service level is 99.5% During a Service Assessment period; the service level achieved is 96.5%:

DKYC & VKYC software~ Rs. 10

crores Software and its licenses ~

Rs. 2 crores

Annual Maintenance Charges and Annual Technical Support ~ Rs. 5 crores

Total Cost of Product and Services billing value for the defaulted period & defaulted deliverable
~ Rs. 17 crores

The Availability Service Credit due to the Bank would be computed as

follows: Minimum Service Level

Monthly Service Level Default = $M1 = 99.5 - 96.5 = 3$

Availability Service Credit for M1 = $3\% * (10 \text{ crores} + 2 \text{ crores} + 5 \text{ crores}) = \text{Rs.} 51,00,000$

Bidder has to note that the total cost of products and services is exclusive of taxes for the purpose of computation of the service level and service credit.

Service Levels during Post implementation phase

The Bidder is expected to complete the new changes / functionalities / responsibilities that have been assigned as per the agreed Change order timelines, for new deliverables Penalty would be levied for implementation delays for new requirement and shall be a maximum of 50% of the total cost of that change solution finalized between the bank and vendor.

Post Implementation Phase Delays	Penalty on total cost of the change solution
1 Week delay from Agreed Timelines	10%
2 Week delay from Agreed Timelines	20%
More than 2 Week delay from Agreed Timelines	50%

If the bidder fails to deliver any or all of the Goods or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% of the of the order value of the product and or services cost per week or part thereof until actual delivery or performance, (above 3 days will be treated as a week); and the maximum deduction

is 50% of the contract value. Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

Tables of Incident Matrix

Incident to be reported within (if unresolved)	Escalation Hierarchy
15 min	Senior Manager
1 hour	Chief Manager
2 hours	Assistant General Manager / Deputy General Manager
> 4 hours	General Manager / Chief General Manager

15.21 Implementation Schedule

Successful bidder should supply, configure, customize, implement, integrate and maintain DKYC & VKYC applications as per scope of work requirement. Bank expects the implementation to be complete within **8 Months** from the date of PO and may be implemented in phases, following are indicative phase:

Phase	Timeline
1. Documentation / project design / implementation plan / interface design with Bank sign off / delivery of software license	within 2 months from release of PO
2. Phase-1: Implementation of any 10 journeys as per Bank's requirement	within 4 months from release of PO; This date will be treated as Project Go-Live. FM Services shall be started after this milestone.
3. Phase-2: Implementation of 10 journeys	within 6 months from release of PO
4. Phase-3: Implementation of 10 journeys	within 8 months from release of PO

Material adverse events:

Successful bidder, during the service period, will have to report material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) And the incidents required to be reported to the bank to enable bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.

Effective access by bank to all record:

Bank should have effective access to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the successful bidder during the period of contract.

Successful bidder to provide details of data:

The successful bidder to provide to bank the details of data (related to bank and its customers) captured, processed and stored.

Data / information which can be shared:

The successful bidder is not permitted to share any types of data/information/customer data/information with bank's customer and / or any other party. The successful will be comply by the digital personal data protection act, 2023 (DPDP Act) and amendments thereon.

Contingency plans:

Successful bidder should have a contingency plan(s) to ensure business continuity and testing requirements.

Information of third parties:

Bank will have right to seek information from the successful bidder about the third parties (in the supply chain) engaged by the former.

Prior approval / consent of bank for use of sub- contractors:

Successful bidder to take prior approval/ consent of the bank for use of sub-contractors for all or part of an outsourced activity.

Skilled resources of successful bidder for core services:

Successful bidder to have provision to consider its skilled resources who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);

Back to back arrangements between successful bidder and OEM:

There should be suitable back-to-back arrangements between successful bidder and the OEMS, if any.

No relationship of master and servant or employer and employee

Notwithstanding what is stated elsewhere in this agreement, there will not be any relationship of master and servant or employer and employee as between the bank on the one hand and the successful bidder and/or the personnel employed/engaged by the successful bidder on the other hand.

Sustainable sourcing:

The supplier shall adhere to sustainable sourcing practices including but not limited to the use of environment friendly materials, ethical labor practices and compliance with relevant local and international regulations. The supplier shall provide documentation or certifications demonstrating their commitment to sustainable sourcing upon request. Failure to comply with these requirements may result in contract termination.

INFORMATION SECURITY

Successful Bidder upon selection will comply with all the present and future provisions of the Information Security Policy of the Bank / Guidelines of RBI, Respective Govt. Agencies and the Bank and provide such regulatory requirements or compliance to Bank during the contract period. The Solution may be audited by RBI/any other Regulatory Authority and any observation pointed out by these bodies have to be complied by the successful bidder within the timelines stipulated by the regulatory agencies, without any additional cost to the Bank. The offered solution shall be subjected to Bank's audit through off-site and on-site scrutiny at any time during the contract period. The auditors may be internal/ external. The successful bidder should provide solution and implementation for all the audit points raised by Bank's internal/external team during the contract period, within the stipulated timelines, without any extra cost. Software solution provided by the bidder must be bug free and confirmation for the same have to be submitted from the respective OEM. Details of Bank's latest IT Security Policy shall be shared with the successful bidder for the implementation and compliance of the policy and guidelines.

Confidentiality & Non – Disclosure

The bidder is bound by this agreement for not disclosing the Banks data and other information. Resources working in the premises of the Bank are liable to follow the rules and regulations of the Bank and are governed by the outsourcing policy of the Bank.

The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to the internal business and operational information of the Bank, affiliates, and/or business partners, disclosure of receipt

of this tender or any part of the aforementioned information to parties not directly involved in providing the requested services could result in the disqualification of the bidders, premature termination of the contract, or legal action against the bidder for breach of trust.

No news release, public announcement or any other reference to the order, relating to the contracted work if allotted with the assignment or any program hereunder shall be made without written consent from the Bank.

As the bidder is providing support services for multiple Banks, the bidder at all times should take care to build strong safeguards so that there is no mixing together of information/documents, records and assets is happening by any chance.

The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts.

The Non-Disclosure Agreement (NDA) should be entered in to between the Bank and the successful bidder within a period of 21 days from, the date of acceptance of purchase order.

Guarantee on software license

The bidder shall guarantee that the software and License supplied under this contract to the Bank is legally obtained. Software supplied should not have any embedded malicious and virus programs.

Force Majeure

The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the parties, as a result of force majeure. For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the parties, due to or as a result of or caused by acts of God, wars, epidemic/pandemic, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.

In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within five calendar days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavor to find a solution to the problem.

Notwithstanding above, the decision of the Bank shall be final and binding on the Bidder.

Resolution of Disputes

The Bank and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, the Bank and the Bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract, shall be referred to two Arbitrators: one Arbitrator to be nominated by the Bank and the other to be nominated by the Bidder.

In the case of the said Arbitrators not agreeing, then the matter will be referred to an umpire to be appointed by the Arbitrators in writing before proceeding with the reference. The award of the Arbitrators, and in the event of their not agreeing, the award of the Umpire appointed by them shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai.

The Language of Arbitration will be English. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, bidder will continue to perform its contractual obligations and the Bank will continue to pay for all products and services that are accepted by it, provided that all products and services are serving satisfactorily, as per satisfaction of the Bank.

If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission, by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) on the date of acknowledgment signed by the receiver or (iii) the business date of receipt, if sent by courier.

This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP. Notwithstanding the above, The Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.

Successful Bidder's liability

The Bidders aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract. The Bidders liability in case of claims against the Bank resulting from misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of **any third-party** patents, trademarks, copyrights (if any) or breach of confidentiality obligations shall be unlimited. In no event shall the Bank be liable for any indirect, incidental or consequential damages or

liability, under or in connection with or arising out of this tender and subsequent agreement or services provided. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

Inspection, Audit, Review, Monitoring & Visitations

All records of OEMs/Bidders with respect to any matters / issues covered under the scope of this RFP/project shall be made available to the Bank at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Such records are subject to examination. The Bank's auditors would execute confidentiality agreement with the Bidder, provided that the auditors would be permitted to submit their findings to the Bank, which would be used by the Bank. The cost of such audit will be borne by the Bank. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/BIDDER outsourced process to identify new outsourcing risks as they arise. The BIDDER shall be subject to risk management and security and privacy policies that meet the Bank's standard. In case the BIDDER outsourced to third party, there must be proper Agreement / purchase order with concerned third party. The Bank shall have right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations. Access to books and records/Audit and Inspection would include:

- a) Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the BIDDER. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.
- b) Provide the Bank with right to conduct audits on the BIDDER whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the bank.
- c) Include clause to allow the Reserve Bank of India or persons authorized by it to access the bank's documents: records of transactions, and other necessary information given to you, stored or processed by the BIDDER within a reasonable time. This includes information maintained in paper and electronic formats.
- d) Recognized the right of the Reserve Bank of India to cause an inspection to be made of a service provider of the bank and its books and account by one or more of its officers or employees or other persons.

Banks shall at least on an annual basis, review the financial and operational condition of the BIDDER. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the BIDDER. Such assessment and reports on the BIDDER may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.

Monitoring

Compliance with Information security best practices may be monitored by periodic Information security audits performed by or on behalf of the Bank and by the RBI. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited

to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, network security controls and program change controls. To the extent that the Bank deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Service Provider shall afford the Bank's representatives access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Bidder must provide the Bank access to various monitoring and performance measurement systems (both manual and automated). The Bank has the right to get the monitoring and performance measurement systems (both manual and automated) audited without prior approval /notice to the Bidder.

Visitations

The Bank shall be entitled to, either by itself or its authorized representative, visit any of the Bidder's premises without prior notice to ensure that data provided by the Bank is not misused. The Bidder shall cooperate with the authorized representative(s) of the Bank and shall provide all information/ documents required to the Bank.

Termination

Termination for Default: The Bank, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Successful Bidder, may terminate this Contract in whole or in part:

- i) If the Successful Bidder fails to deliver any or all of the deliverables / milestones within the period(s) specified in the Contract, or within any extension thereof granted by the Bank; or;
 - ii) If the Successful Bidder fails to perform any other obligation(s) under the contract.
 - iii) If the Successful Bidder, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract. Corrupt practice means the offering, giving, receiving or soliciting of anything of value or influence the action of a public official in the procurement process or in contract execution; and "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank, and includes collusive practice among Bidders (prior or after bid submission) designed to establish bid prices at artificial non- competitive levels and to deprive the Bank of the benefits of free and open competition.
- b) In the event, the Bank terminates the Contract in whole or in part, the Bank may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Successful Bidder shall be liable to the Bank for any excess costs for such similar Goods or Services. However, the Successful Bidder shall continue performance of the Contract to the extent not terminated when the value of the liquidated damages exceed 10% of the contract value.
 - c) In case the contract is terminated then all undisputed payment will be given to bidder, but disputed payment shall be adjusted by way of penalty from invoices or PBG.

Termination for Insolvency: If the Bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Bidder is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Bidder takes or suffers any other analogous action in consequence of debt; then the Bank plans to, at any time, terminate the contract by giving written notice to the Bidder. If the contract is terminated by the Bank in terms of this Clause, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Bank. In case, the termination occurs before implementation in all the locations in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the Bidder.

Termination – Key Terms & Conditions: The Bank reserves the right to terminate the agreement with the Bidder / bidder at any time by giving ninety (90) days prior written notice to the Bidder. The Bank shall be entitled to terminate the agreement at any time by giving notice if the Bidder.

- i) has a winding up order made against it; or
- ii) has a receiver appointed over all or substantial assets; or
- iii) is or becomes unable to pay its debts as they become due; or
- iv) enters into any arrangement or composition with or for the benefit of its creditors; or
- v) Passes a resolution for its voluntary winding up or dissolution or if it is dissolved.

The Bidder shall have right to terminate only in the event of winding up of the Bank.

Exit Option and Contract Re-Negotiation:

- (a) The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:
 - i) Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 21 days of receipt of purchase contract.
 - ii) Delay in delivery, performance or implementation of the solution beyond the specified period;
 - iii) Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of The Bank. Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by The Bank. (60 days will be construed as the notice period)
- (b) In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.

Corrupt and Fraudulent Practices

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution AND

"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of The Bank and includes collusive practice among Bidders (prior to or after offer submission) designed to establish offer prices at artificial non-competitive levels and to deprive The Bank of the benefits of free and open competition.

The Bank reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question. The Bank reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

All necessary compliances relating to the transaction such as disclosure in in the returns to be filed, Tax Collected at Source (if applicable) etc. shall be duly undertaken by the supplier and in case of any non-compliance or delayed compliance, the Bank shall have right to recover interest and/or penalty that may be levied including liquidated damages @10 % of the value of supplier.

This indemnification is only a remedy for the Bank. Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above.

Entire Agreement; Amendments

This Agreement sets forth the entire agreement between the Bank and the Successful bidder and supersedes any other prior proposals, agreements and representations between them related to its subject matter, whether written or oral. No modifications or amendments to this Agreement shall be binding upon the parties unless made in writing, duly executed by authorized officials of both parties.

Survival and Severability

Any provision or covenant of the Agreement, which expressly, or by its nature, imposes obligations on successful bidder shall so survive beyond the expiration, or termination of this Agreement. The invalidity of one or more provisions contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof; and in the event that one or more provisions shall be declared void or unenforceable by any court of competent jurisdiction, this Agreement shall be construed as if any such provision had not been inserted herein.

Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Document. Submission of a bid not responsive to the Bidding Document in every respect will be at the bidder's risk and may result in the rejection of its bid without any further reference to the bidder.

Amendments to Bidding Documents

At any time prior to the last Date and Time for submission of bids, the Bank may, for any reason, modify the Bidding Document by amendments at the sole discretion of the bank. All amendments will be **either uploaded in the website** or shall be delivered by hand / post / courier or through e-mail or faxed to all prospective bidders, who have received the bidding document and will be binding on them. For this purpose, bidders must provide name of the contact person, mailing address, telephone number and FAX numbers on the covering letter sent along with the bids.

In order to provide, prospective bidders, reasonable time to take the amendment if any, into account in preparing their bid, the Bank may, at its discretion, extend the deadline for submission of bids.

Period of Validity

Bids shall remain valid for 180 days from the last date of bid submission. A bid valid for shorter period shall be rejected by the bank as non-responsive.

Last Date and Time for Submission of Bids

Bids must be submitted not later than the specified date and time as specified in the Bid Document. Bank reserves the right to extend the date & time without mentioning any reason.

Modifications and/or Withdrawal of Bids

- a) Bids once submitted will be treated as final and no further correspondence will be entertained on this.
- b) No bid will be modified after the deadline for submission of bids.
- c) No bidder shall be allowed to withdraw the bid, if the bidder happens to be a successful bidder.

Clarifications of Bids

To assist in the examination, evaluation and comparison of bids the bank may, at its discretion, ask the bidder for clarification and response, which shall be in writing and without change in the price, shall be sought, offered or permitted.

Bank's Right to Accept or Reject Any Bid or All Bids

The bank reserves the right to accept or reject any bid and annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability

to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the ground for the bank's action.

Preference to Make in India

Government has issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P-45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 28.05.2018, 29.05.2019, 04.06.2020 and dated 16-9-2020 to encourage 'Make in India' and to promote manufacturing and production of goods, services and works in India with a view to enhancing income and employment.

It is clarified that for all intents and purposes, the latest revised order i.e. the order dated 16-9-2020 shall be applicable being revised Order of the original order i.e. Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 dated 15-6-2017.

The salient features of the aforesaid Order are as under:

1. **Class-I Local supplier** – a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%
2. **Class-II Local supplier** – a supplier or service provider, whose goods, services or works offered for procurement, has local content more than 20% but less than 50%.
3. **Non-Local supplier** – a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%.
4. **The margin of purchase preference shall be 20%.**, Margin of purchase preference means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference.
5. **"Minimum Local content"** for the purpose of this RFP, the 'local content' requirement to categorize a supplier as 'Class-I local supplier' is minimum 50%. For 'Class-II local supplier', the 'local content' requirement is minimum 20%. If Nodal Ministry/Department has prescribed different percentage of minimum 'local content' requirement to categorize a supplier as 'Class-I local supplier'/'Class-II local supplier', same shall be applicable.

Verification of Local contents:

2. The local supplier at the time of submission of bid shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content as per Annexure-16. Local content certificate shall be issued based upon the procedure for calculating the local content /domestic value addition on the basis of notification bearing no. F. No.33(1)/2017-IPHW dated 14-9-2017 issued by Ministry of Electronics and Information Technology read with Public Procurement (Preference to Make in India) Order 2017 Revised vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No. P- 45021/2/2017-B.E.-II dated 16-09-2020
3. False declaration will be in breach of the Code of Integrity under Rule 175(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to

two years as per rule 151 of the General Financial Rules along with such other actions may be permissible under law.

4. A supplier who has been debarred by any procuring entity for violation of this order shall not be eligible for preference under this order for procurement by any other procuring entity for the duration of the debarments. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities in the manner prescribed under order No P-45021/2/2017-PP(BE-II) dated 16-09-2020, para 9(h).

Violation of Terms

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained under the RFP/Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

Independent Contractor

Nothing herein contained will be construed to imply a joint venture, partnership, principal-agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/ NDA (Non-Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labor laws for its employees and sub-contractors or as the case may be. Bidder should take bank's prior written permission before subcontracting/ resource outsourcing of any work related to the performance of this RFP or as the case may be. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

Indemnity

- a) The Bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses,

liabilities, claims, actions, costs and expenses (including attorney's fees) relating to,
 - resulting directly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:

- i) Bank's authorized/Bonafide use of the Deliverables and/or the Services provided by Bidder under this RFP or any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - ii) An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP or, any or all terms and conditions stipulated in the SLA (Service level Agreement) or Purchase Order (PO) and/or
 - iii) Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank and/or
 - iv) Breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Bidder under this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - v) Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights and/or
 - vi) Breach of confidentiality obligations of the Bidder contained in this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
 - vii) Negligence or gross misconduct attributable to the Bidder or its employees, agent or sub-contractors.
- b) The Bidder will have to at its own cost and expenses defend or settle any claim against the Bank that the Deliverables and Services delivered or provided under this RFP infringe IPR (Intellectual Property Right) such as patent, utility model, industrial design, copyright, trade secret, mask work or trade mark etc. in the country where the Deliverables and Services are used, sold or received, provided the Bank:
- i) Notifies the Bidder in writing; and
 - ii) Cooperates with the Bidder in the defense and settlement of the claims.
- c) The Bidder shall compensate the Bank for direct financial loss suffered by the Bank, if the Bidder fails to fix bugs, provide the Modifications / Enhancements / Customization as required by the Bank as per the terms and conditions of this RFP and to meet the Service Levels as per satisfaction of the Bank.
- d) Additionally, the Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, suffered by bank due to the following reasons:
- i) that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or

trademark in any country where the Deliverables and Services are used, sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.

- ii) all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or
- iii) such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:
 - (a) The Bidder has sole control of the defense and all related settlement negotiations.
 - (b) The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.
 - e) Indemnity would be limited to damages awarded in arbitration and shall exclude indirect, and incidental damages. However, indemnity would also cover damages, loss or liabilities, compensation suffered by the Bank arising out of claims made by regulatory authorities.

18.17 Digital Personal Data Protection Compliance

The Bidder/Vendor shall, always, comply with the provisions of the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 / Notifications / Guidelines and further rules made thereunder. The Bidder/Vendor shall implement appropriate technical and organizational measures to ensure lawful processing, secure handling, confidentiality, integrity, availability, and protection of personal data obtained, accessed, shared, or processed in connection with this RFP and the resultant contract.

Further, the Bidder/Vendor shall take due care while collecting and dealing with sensitive personal data or information of Bank and its customer. Any processing of Personal Data by the Service Providers in the performance of the Agreement under this RFP shall be following the above Act/Rules. The Service Provider shall also ensure that any sub-contractor (if allowed) engaged by it shall act in compliance with the above Act, to the extent applicable.

The Bidder/Vendor shall act only on documented instructions of the Bank and shall not process personal data for any purpose other than the performance of the obligations under this RFP.

Any data breach, unauthorized access, misuse, loss, or disclosure of personal data must be reported to the Authority/Bank in writing within [24 hours] of occurrence, along with an incident report and remedial action plan.

The Bidder/Vendor shall indemnify and hold harmless the Bank against any loss, liability, penalty, claim, cost, or damages arising out of non-compliance with the DPDP Act and Rules.

18.18 Labor Law Adherence and Compliance with Court Directions

The Bidder/Vendor shall ensure full compliance with all applicable labour laws, employment laws, industrial relations regulations, social security legislation, and any orders/directions issued by competent Labour Courts/Industrial Tribunals/Authorities / RBI and any other Regulatory/ Statutory body in India.

The Bidder/Vendor shall be solely responsible for payment of salaries, wages, statutory contributions, benefits, and all dues to its employees, subcontractors, labour, and statutory personnel deployed for execution of work under this RFP.

No employer-employee relationship shall be deemed to exist between the Bank and the personnel engaged by the Bidder/Vendor.

In case of any claim, demand, dispute, or litigation arising due to non-compliance by the Bidder/Vendor, the same shall be solely borne and resolved by the Bidder/Vendor without any liability upon the Bank.

The Bidder/Vendor shall indemnify the Bank against any losses, costs, or legal liabilities on account of any violation or non-compliance of applicable laws including any liabilities, costs or expenses arising in connection with any proceedings in respect thereof."

Annexure 1: Conformity Letter:

To,

**Assistant General
Manager - IT Central
Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-
11, CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Further to our proposal dated _____, in response to the RFP document (hereinafter referred to as "RFP DOCUMENT") issued by Central Bank of India ("Bank") we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP document and the related addendums and other documents including the changes made to the original tender documents issued by the Bank.

The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Signature of Authorized
Signatory: Name of Signatory:
Designation:
Seal of Company:

Date:

Place:

Annexure 2: Compliance to Terms & Conditions

To,

**Assistant General
 Manager - IT Central
 Bank of India
 Cent Neo, 6th Floor, Tower No.7
 Belapur Railway Station Complex, Sector-
 11, CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We submit our Bid Document herewith. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bids together with the written acceptance thereof shall constitute a binding contract between us.

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

We undertake that product and services supplied shall be as per the: -

Compliance	Compliance (Yes/ No)
Terms & Conditions	
Scope of Work	

Signature of Authorized
 Signatory: Name of
 Signatory:
 Designation:
 Seal of Company:

Date:

Place:

Annexure 3: Pro-forma for deed of indemnity: *

(need to be stamped as per law)

This deed of Indemnity is made on this the day of, 2026

BETWEEN

M/s. is_a Company incorporated under the Companies Act, 1956/2013 with CIN having its registered office at (Hereinafter referred to as "**the Indemnifier**" which expression shall unless excluded by or repugnant to the context, be deemed to mean and include its assigns, administrators and successors) of the First Part:

AND

Central Bank of India, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chander Mukhi, Nariman Point, Mumbai and among other department of corporate office, CentNeo , 6th Floor, 7th Tower (CBD Railway station) sector 11 CBD Belapur 400614, hereinafter called "**Bank / Indemnified**" which expression shall mean and include, unless the context otherwise requires, its successors) of the Second Part

WHEREAS;

1. The Bank proposes to procure Supply, Procurement, Implementation and Maintenance of Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels as provided in RFP [..... ref details of RFP is to be given], and the indemnifier who participate in the said process explicitly undertook to keep the indemnified/ Bank 'harmless, against all losses, claims, demands and costs without any ceiling but to the actual loss occurred. The law governing this Indemnity would be Indian Law.
2. Indemnifier has qualified to participate in the bid process as per the conditions of the RFP mentioned above. Represented and warranted

that bidders are properly authorized and legally 'competent' and are not debarred / disqualified by any applicable laws, regulations or guidelines for the time being in force.

3. Agreed that on the event of selecting as successful bidder, to install and provide comprehensive maintenance for the equipment, materials used and workmanship by them and execute / submit all the required documents, Performance bank Guarantee, Non- Disclosure Agreement, Integrity Pact, Documents or undertakings by and from OEM/OSD , Service Level Agreement (SLA) etc. in Bank's Format within the time specified.
4. The software /services we are offering is not infringing any of the intellectual Property rights and in case of any such third party claims , legal actions face in relation to this by the Bank, Indemnifier will be responsible to compensate the Bank for all cost incurred/ penalties / compensations .
5. This Indemnity shall be in force till the next indemnity deed executed (if any) by the successful bidder and for all other bidders who participate is for 6 months after the contract has been awarded

In WITNESS THEREOF the indemnifier herein has set their / his hands and seal
, sign and submit to the indemnified.

INDEMNIFIER

Signature of Authorized
Signatory: Name of
Signatory:
Designation:
Seal of Company:

Date:

Place:

Annexure 4: Undertaking of Authenticity for Products Supplied:

To,

**Assistant General
Manager - IT Central
Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-
11, CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

With reference to RFP for Implementation of DKYC & VKYC.

We hereby undertake to produce the certificate from our OEM supplier in support of this undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM suppliers at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at any time, we agree to take back the Licenses without demur, if already supplied and return the money if any paid to us by you in this regard.

Signature of Authorized

Signatory: Name of

Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 5: Undertaking for Acceptance of Terms of RFP.

To,

**Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

With reference to RFP for Implementation of DKYC & VKYC.

We understand that Bank shall be placing Order to the Successful Bidder exclusive of taxes only.

We confirm that in case of invocation of any Bank Guarantees submitted to the Bank, we will pay applicable GST on Bank Guarantee amount.

We are agreeable to the payment schedule as per "Payment Terms" of the RFP.

We here by confirm to undertake the ownership of the subject RFP.

We hereby undertake to provide latest product/ software with latest version. The charges for the above have been factored in Bill of Material (BOM); otherwise, the Bid is liable for rejection. We also confirm that we have not changed the format of BOM.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 6: Manufacturer's / OSD Authorization Form:

To,

**Assistant General Manager - IT Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11, CBD
Belapur, Navi Mumbai- 400614**

Sir

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We (Name of the Manufacturer) who are established and reputable manufacturers of having factories at,,, and do hereby authorize M/s (who is the Bidder submitting its bid pursuant to the Request for Proposal issued by the Bank) to submit a Bid and negotiate and conclude a contract with you for supply of equipment manufactured by us against the Request for Proposal received from your Bank by the Bidder and we have duly authorized the Bidder for this purpose.

We, hereby, extend warranty for the equipment and support services offered for our products supplied against this RFP by the above-mentioned Bidder.

If Bank desires transfer of the warranty and support services, supposed to be delivered by the successful Bidder, to its preferred Bidder, in such a case, OEM should transfer such warranty and support services without any additional cost to the Bank.

The software doesn't infringe any kind of intellectual property rights and in case of claims / suits / legal action by third parties and the cost, penalties, compensation incurred / suffered by the bank will be indemnified

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal:

Date:

Place:

(This letter should be on the letterhead of the Manufacturer duly signed & seal by an authorized signatory)

Annexure 7: Pre- Contract Integrity Pact (need to be stamped as per law)

This Pre- Contract Integrity Pact is made on this the day of 2026

Between

Central Bank of India, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chander Mukhi, Nariman Point, Mumbai and among other department of corporate office, CentNeo , 6th Floor, 7th Tower (CBD Railway station) sector 11 CBD Belapur 400614, hereinafter called "**Bank / Principal**" which expression shall mean and include, unless the context otherwise requires, its successors) of the First Part

And

M/s A company registered under Indian Companies Act 2013, with CIN And having its Registered office at (Full address) represented by Mr. Chief Executive Officer/ Authorized signatory (hereinafter called the "**BIDDER**" which expression shall mean and include, unless the context otherwise requires, its / his successors and permitted assigns of the Second Part.

PREAMBLE

Whereas the principal proposes to procure Supply, Procurement, Implementation and Maintenance of Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels as provided in RFP and under laid down organizational procedures, and for its contracts, the Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s).

Section 1 – Commitments of the Principal

- 1) The principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -
 - a. The Principal/ Bank undertakes that no official of the principal, connected directly or indirectly with the contract, will demand, take a promise for or Accept or attempt to accept , directly or through intermediaries, any bribe, consideration, gift, reward, favor or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, Bid evaluation, contracting or implementation process related to the contract

- b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
 - c. The Principal will exclude all known prejudiced from the process. All the officials of the Principal will report to the appropriate authority any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach
- (2) If the Principal obtains information on the misconduct of any of its employees with full and verifiable facts and the same is prima facie found to be correct by the principal, the principal will inform the Chief Vigilance Officer or to any competent authority as per law and in addition can initiate disciplinary actions and such a person shall be debarred from further dealings related to the contract process. However in such situation proceedings under the contract would not be stalled.
- (3) In order to achieve these goals, the principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 2 – Commitments of the Bidder(s)

The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

- (1) The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any materials or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the Contract.
- (2) The BIDDER further undertakes that it has not given, offered or promised to give, directly or Indirectly any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission fees, brokerage or inducement to any official of the PRINCIPAL or otherwise in procuring the Contract or for bearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Central bank of India for showing or forbearing to show favor or disfavor to any person in relation to the contract or any other contract with Central bank of India. BIDDERS shall disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principals or associates. The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract. The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair

means and illegal activities. The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the PRINCIPAL as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged. The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts. The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above. If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the PRINCIPAL, or alternatively if any relative of an officer of the PRINCIPAL has financial interest /stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the PRINCIPAL.

SECTION 3 - DISQUALIFICATION FROM TENDER PROCESS AND EXCLUSION FROM FUTURE CONTRACTS

If the BIDDER, before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the principal is entitled to disqualify the BIDDER from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". A copy of the "Guidelines on Banning of business dealings" is provided in Annexure-17 of the RFP.

SECTION 4 – COMPENSATION FOR DAMAGES

1. If the Principal has disqualified the Bidder from the tender process prior to the award according to Section 3 of Integrity Pact, the Principal is entitled to demand and recover the damages equivalent to earnest money deposit/ bid security, as referenced in the RFP.
2. If the Principal has terminated the contract according to Section 3, or if the principal is entitled to terminate the contract according to Section 3 of Integrity Pact, the principal shall be entitled to demand and recover from the BIDDER liquidated damages of the contract value or the amount equivalent to the performance bank guarantee, as referenced in the RFP.

SECTION 5 – PREVIOUS TRANSGRESSION

1. The Bidder declares that no previous transgressions occurred in the last three years with any other bank in any country conforming to the anti-corruption approach or with any public sector enterprise in India that could justify his exclusion from the tender process.

2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

SECTION 6 – EQUAL TREATMENT OF ALL BIDDERS / SUBCONTRACTORS

1. The Bidder undertakes to demand from his subcontractors a commitment in conformity with this Integrity Pact.
2. The principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.
3. The principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

SECTION 7 – CRIMINAL CHARGES AGAINST VIOLATING BIDDER(S) / CONTRACTOR(S) / SUBCONTRACTOR(S)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the principal has substantive suspicion in this regard, the Principal will inform the same to the CVO of the Bank or to any such competent authorities or law enforcing agencies.

SECTION 8 – INDEPENDENT EXTERNAL MONITOR / MONITORS

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders as confidential.
3. The Bidder accepts that the Monitor has the right to access without restriction to all Project documentation of the principal including that provided by the Bidder The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder/ Contractor/ Subcontractor with confidentiality. In case of sub-contracting, the Principal Contractor shall take all responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-contracting, the

Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.

4. The principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Bidder. The parties offer to the Monitor the option to participate in such meetings.
5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.
6. The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.
7. If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant BNS/ IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the CVO, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
8. The word "Monitor" would include both singular and plural.

SECTION 9 - PACT DURATION

This Pact begins when both parties have legally signed it. It expires for the Bidder 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman & Managing Director of CENTRAL BANK OF INDIA.

SECTION 10 - OTHER PROVISIONS

1. This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e., Mumbai City.

2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
4. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

SECTION 11- FALL CLAUSE

The BIDDER undertakes that it has not supplied/is not supplying same/exact product/systems or subsystems/services (i.e. same scope, deliverables, timelines, SLAs & pricing terms) at a price lower than that offered in the present bid to any other bank or public sector undertaking or government department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER to any other bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the Bank, if the contract has already been concluded.

BANK/PRINCIPAL
Name, Designation, Office address
OVD Number

BIDDER
Name, Designation, office address
OVD Number

Witness:

- 1.
- 2.

Annexure 8: Non-Disclosure Agreement:

This Agreement made at _____, on this ____ day of ____ 2026.

Between

a company incorporated under the Companies Act, 1956/2013 having its registered office at _____ (hereinafter referred to as "-----" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the ONE PART;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office, Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as "BANK" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the OTHER PART

The _____ bidder and BANK are hereinafter individually referred to as party and collectively referred to as "the Parties". Either of the parties which discloses or receives confidential information are respectively referred to herein as Disclosing Party and Receiving Party.

WHEREAS:

The Parties intend to engage in discussions and negotiations concerning the establishment of a business relationship between them. In the course of such discussions and negotiations, it is anticipated that both the parties may disclose or deliver to either of the Parties certain or some of its trade secrets or confidential or proprietary information, for the purpose of enabling the other party to evaluate the feasibility of such business relationship (hereinafter referred to as "the Purpose").

NOW, THEREFORE, THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

Confidential Information

"Confidential Information" means all information disclosed/ furnished by either of the parties to another Party in connection with the business transacted/to be transacted between the Parties and/or in the course of discussions and negotiations between them in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof.

Either of the Parties may use the Confidential Information solely for and in connection with the Purpose.

Notwithstanding the foregoing, "Confidential Information" shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly available without breach of this Agreement by the Receiving Party,

(b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, or (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

Non-Disclosure

The Receiving Party shall not commercially use or disclose any Confidential Information, or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to its employees, consultants, auditors, sub-contractors ("Representatives") consultants only if such representatives have executed a Non-Disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefor.

Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

Publications

Neither Party shall make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the other Party.

Term

This Agreement shall be effective from the date hereof and shall continue till establishment and completion of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease rights to any and all disclosures or uses of Confidential Information; and at the request of the Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

Notwithstanding anything to the contrary contained herein, the confidential information shall continue to remain confidential until it reaches the public domain in the normal course.

Title & Proprietary Rights

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice,

confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other mark, symbol or logo on such Confidential Information.

Return of Confidential Information

Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph. The obligation under this clause will not apply where it is necessary to retain any confidential information for the purpose as required by the law or for internal auditing purposes or electronic data stored due to automatic archiving or backup procedures.

Remedies

The Receiving Party acknowledges that if the Receiving Party fails to comply with any of its obligations hereunder, the Disclosing Party may suffer immediate, irreparable harm for which monetary damage may not be adequate. The Receiving Party agrees that, in addition to all other remedies provided at law or in equity, the Disclosing Party shall be entitled to injunctive relief hereunder.

Entire Agreement, Amendment and Assignment

This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

Governing Law and Jurisdiction

The provisions of this Agreement shall be governed by the laws of India. The disputes, if any, arising out of this Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai City.

General

The Receiving Party shall not reverse-engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder. All Confidential Information is provided "as is". In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by the parties constitutes any representation, warranty, assurance, guarantee or inducement by either party to the other with respect to the fitness of such Confidential Information for any particular purpose or infringement of trademarks, patents, copyrights or any right of third persons.

Indemnity

The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party, its officers, employees or consultants.

In WITNESS THEREOF, the Parties hereto have executed these presents the day, month and year first

hereinabove written:

Signed, Sealed and Delivered for the Principal	Signed, Sealed and Delivered for the Bidder
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____
Company Seal	Company Seal

Witness I	Witness II
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____

Annexure 9: Performance Bank Guarantee (PBG):

To,

Central Bank of India

Mumbai

In consideration of Central Bank of India having Registered Office at Chander Mukhi Building, Nariman Point, Mumbai 400 021 (hereinafter referred to as "Purchaser") having agreed to purchase of software, hardware & other components & services (hereinafter referred to as "Goods") from M/s -----(hereinafter referred to as "Contractor") on the terms and conditions contained in their agreement/purchase order No----- dt.----- (hereinafter referred to as the "Contract") subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the complete DKYC & VKYC Platform and Solution, as per the terms and conditions of the said contract, to be supplied by the contractor and also guaranteeing the maintenance, by the contractor, of the computer hardware and systems as per the terms and conditions of the said contract;

1) We, -----(Bank) (hereinafter called "the Bank"), in consideration of the premises and at the request of the contractor, do hereby guarantee and undertake to pay to the purchaser, forthwith on mere demand and without any demur, at any time up to ----- any money or moneys not exceeding a total sum of ₹----- (Rupees -----only) as may be claimed by the purchaser to be due from the contractor by way of loss or damage caused to or that would be caused to or suffered by the purchaser by reason of failure of computer software / hardware to perform as per the said contract, and also failure of the contractor to maintain the computer software / hardware and systems as per the terms and conditions of the said contract.

2) Notwithstanding anything to the contrary, the decision of the purchaser as to whether computer software / hardware has failed to perform as per the said contract, and also as to whether the contractor has failed to maintain the DKYC & VKYC Platform and Solution as per the terms and conditions of the said contract will be final and binding on the Bank and the Bank shall not be entitled to ask the purchaser to establish its claim or claims under this Guarantee but shall pay the same to the purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the contractor. Any such demand made by the purchaser on the Bank shall be conclusive and binding notwithstanding any difference between the purchaser and the contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3) This Guarantee shall expire on -----; without prejudice to the purchaser's claim or claims demanded from or otherwise notified to the Bank in writing on or before the said date i.e.----- (this date should be date of expiry of Guarantee).

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue

to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the purchaser under or by virtue of the said contract have been duly paid and its claims satisfied or discharged or the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the purchaser that the purchaser shall have the fullest liberty without affecting in any manner the Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the purchaser against the contractor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and the Bank shall not be released from its liability for the reasons of any such extensions being granted to the contractor for any forbearance, act or omission on the part of the purchaser or any other indulgence shown by the purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the contractor or the Bank nor shall it be affected by any change in the constitution of the purchaser by any amalgamation or absorption or with the contractor, Bank or the purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by us (whether singly or jointly with other banks) on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing un-cancelled and we further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by us on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to our local address as mentioned in this guarantee.

Notwithstanding anything contained herein above: -

i) Our liability under this Bank Guarantee shall not exceed ₹----- /- (Rupees-----
-only).

ii) This Bank Guarantee shall be valid up to-----; (date of expiry of PBG) and

iii) We are liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before (date of expiry of PBG plus claim period, if any)

10) The Bank has power to issue this Guarantee under the statute/constitution, and the undersigned has full power to sign this Guarantee on behalf of the Bank.

Date this -----day of -----2026 at -----

For and on behalf of ----- Bank.

Sd/- -----

Annexure 10: Pro-forma for Bid Security (EMD):

To,

**Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

In response to your invitation to bid for Procurement and Implementation of DIGITAL KYC and VIDEO KYC Solutions, M/s _____ having their registered office at _____ (hereinafter called the "Bidder") wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

Whereas the "Bidder" has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantees an amount of ₹40,00,000.00 (Rupees Forty Lakh Only) as bid security as required to be submitted by the "Bidder" as a condition for participation in the said process of RFP.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

1. If the Bidder withdraws his proposal during the period of the proposal validity; or
2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal, fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently. We undertake to pay immediately on demand to Central Bank of India the said amount of Rupees 40,00,000.00 without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by Central Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein:

1. Our liability under this Bank guarantee shall not exceed ₹40,00,000.00 (Rupees Forty Lakh Only)
2. This Bank guarantee will be valid up to _____; and
3. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only upon service of a written claim or demand by you or before _____

In witness where of the Bank, through the authorized officer has sets its hand and stamp
on this _____day of _____at.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 11: Letter for Refund of EMD:

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Subject: Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels - Letter for Refund of EMDs

We (Company Name) participated in the Request for Proposal RFP for Procurement, Implementation and Maintenance of Solution for Customer Onboarding through DIGITAL KYC, VIDEO KYC and other channels, and we are an unsuccessful bidder.

Kindly refund the EMD submitted for participation. Details of EMD submitted are as follows:

Sr. No.	Bidder Name	DD/BG Number	Drawn on Bank Name	Amount (₹)

Bank details to which the money needs to be credited via NEFT are as follows.

Name of the Bank with Branch:

Account Type:

Account Title:

Account Number:

IFSC Code:

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 12: NPA Undertaking:

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

**Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We _____(bidder name), hereby undertake that-

We have not been declared NPA by any Bank in India.

Further, we do not have any pending case with any organization across the globe which affects our credibility to service the bank.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 13: Undertaking letter - Land Border Sharing:

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

**Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We, M/s _____ are a private/ public limited company/ LLP/ firm <strike off whichever is not applicable> incorporated under the provisions of the Companies Act, 1956/2013, Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having our registered office at _____ (referred to as the "Bidder") are desirous of participating in the Tender Process in response to our captioned RFP and in this connection we hereby declare, confirm and agree as follows:

We, the Bidder have read and understood the contents of the RFP and Office Memorandum & the Order (Public Procurement No.1) both bearing no.F.No.6/18/2019/PPD of 23rd July 2020 issued by Ministry of Finance, Government of India on insertion of Rule 144 (xi) in the General Financial Rules (GFR) 2017 and the amendments & clarifications thereto, regarding restrictions on availing/ procurement of goods and services, of any Bidder from a country which shares a land border with India and/ or sub-contracting to contractors from such countries.

In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), we, the Bidder hereby declare and confirm that:

Strike off whichever is not applicable.

"I/we have read the clause regarding restrictions on procurement from a bidder of the country w h i c h s h a r e s a land border with India; I/we certify that _____ is not from such a country.

"I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that _____ is from such a country. I hereby certify that _____ fulfils all requirements in this regard and is eligible to be

considered. [Valid registration by the Competent Authority is attached]"

Further, in case the work awarded to us, I/we undertake that I/we shall not subcontract any of assigned work under this engagement without the prior permission of Bank.

Further, we undertake that I/we have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that our subcontractor is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that our subcontractor fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority]"

We hereby confirm that we fulfil all the eligibility criteria as per the office memorandum/ order mentioned above and RFP and we are eligible to participate in the Tender process. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the contract, Bank shall be within its rights to forthwith terminate the contract/ bid without notice to us and initiate such action including legal action in accordance with law. Bank shall also be within its right to forfeit the security deposits/ earnest money provided by us and also recover from us the loss and damages sustained by the Bank on account of the above.

This declaration cum Undertaking is executed by us through our Authorized signatory/ ies after having read and understood the Office Memorandum and Order including the words defined in the said order.

Dated this _____ by _____ 2026

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Bidder's Corporate Name:

Address:

Email & Phone No.:

List of documents enclosed:

Copy of Certificate of valid registration with the Competent Authority (strike off if not applicable)

Date:

Place:

Annexure 14: List of Hardware and Software Components:

To,

Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: List of Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels.

The software below is proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below licenses (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr No.	Software / Tool or Component Required	OEM Name	Justification (Why Software is needed)	Licensing Metric for software (Customer based/ Processor Based/ any other)

The below Hardware items are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below items (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr No.	Hardware Item or Component Required	Quantity	OEM Name	Size of Hardware for provisioning Racks space	Number of Power Inputs and Power consumption for device

In case the hardware to be provided by the Bank, the hardware will be on prem with S390X

architecture on IBM LinuxOne Zsystems, Operating system – RHEL on IBM LinuxOne, Microservices / Kubernetes – Red Hat OpenShift Container Platform, DevSecOps – GITLAB, Database – Oracle DB. Only Oracle License will be provided by the Bank, Installation, Configuration, Maintenance and Backup will be performed by the successful bidder.

The sizing of hardware / Software must be based on current average and peak volume of transactions, oversizing of hardware and the same is under-utilized will lead to penalties.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 15: Cover Letter:

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

To,

**Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Having examined the Scope Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, install and maintain all the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.

If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.

We agree to abide by this bid Offer for 180 days from date of bid (Commercial Bid) opening and our Offer shall remain binding on us which may be accepted by the Bank any time before expiry of the offer.

This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We certify that we have provided all the information requested by the bank in the format prescribed for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 16: Bidder's Particulars on Company Letter Head:

To,

Assistant General Manager - IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Sl. No	Particulars	Details
1	Name of the Bidder	
2	Address with E mail id, Mobile no. and Pin code	
3	GST Number	
4	Bank Details	
5	PAN Number	
6	Name of Authorized Person	
	Mobile No:	
	Landline No:	
7	i. Email ID	
	ii. Alternative Email ID	
8	Details of EMD	BG/UTR/Reference No. date & Amount
9	Exemption Certificate details (if applicable). E.g.: MSME/Udyog Aadhar certificate etc.	Please upload copy of the same along with details
10	Annual Turnover (In Rs.) 2022-23 – 2023-24 – 2024-25 –	
11	Operating Profit (In Rs.) 2022-23 – 2023-24 – 2024-25 –	

12	Net Worth (In Rs.) 2022-23 – 2023-24 – 2024-25 –	
13	Whether all RFP terms & conditions complied with.	

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 17: Guidelines on banning of business dealing:

1) GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

- a) There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with CENTRAL BANK OF INDIA shall apply for registration in the prescribed Application –Form.
- b) Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by CENTRAL BANK OF INDIA.
- c) Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e., Principal) before finalizing the order

2) DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA. IF ANY.

- a) Tenderers of Foreign nationality shall furnish the following details in their offer:
 - 1) The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the principals. In case the agent/representative be a foreign Bank, it shall be confirmed whether it is real substantial Bank and details of the same shall be furnished.
 - 2) The amount of commission/remuneration included in the quoted price(s) for such agents/representatives in India.
 - 3) Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by CENTRAL BANK OF INDIA in Indian Rupees only.
- b) Tenderers of Indian Nationality shall furnish the following details in their offers:
 - The name and address of the foreign principals indicating their nationality as well as their status, i.e., whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.
 - The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.
 - Confirmation of the foreign principals of the Tenderer that the

commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items.

- In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.
- Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by CENTRAL BANK OF INDIA. Besides this there would be a penalty of banning business dealings with CENTRAL BANK OF INDIA or damage or payment of a named sum.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 18: Proposed Team Profile:

To,

Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

S.NO	Job Profile as per RFP	Name of team member	Qualification & certification	Previous Organization where team member was associated	Duration of team member association	No. of years of experience

We hereby acknowledge that the information provided by us is true and to the Best of our Knowledge

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 19: Format for Submission of Client References by Bidder.

To,

Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Particular	Details
Client Information	
Client Name	
Client Address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
• Name of the Project	
• Description of the project	
• Implementation Start Date	
• Implementation End Date	
• Support & Maintenance Start Date	
• Support & Maintenance End Date	
Current Status (In Progress / Completed)	
Size of Project	



Names of Modules Implemented-	
1. Collections	
2. Payments	
3. Mandates	
4. Liquidity Management	
5. Receivables Management	
6. Common Services	
7. Government Business	
Any other information on the Client Reference	

The documentary proof of the client reference is enclosed.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 20: Query Format:

To,

**Assistant General Manager-IT
(Digital) Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Queries:

Sr. No.	Page #	Point / Section #	Query	Banks Response (Bidder Should not fill in this column)
1				
2				
3				
4				
5				
6				
7				
8				
9				

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 21: Eligibility Criteria Compliance:

To,

**Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

Bidder needs to comply with the eligibility criterion mentioned below. Non-compliance with any of these criteria would result in outright rejection of bidder's proposal. Bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labeled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of Bank pertaining to Eligibility Criteria evaluation would be final and binding on all the bidders. Bank may accept or reject an offer without assigning any reason whatsoever.

SL No	Criteria	Proof of documents to be submitted
1.	Bidder should be a limited company (Public/Private) registered in India under the Companies Act, 1956/2013 for the last 3 years as on bid submission date.	1. Certificate of Incorporation issued by Registrar of Companies along with 2. Copies of Memorandum of Association 3. Copies of Articles of Association 4. Shareholding pattern 5. Board Resolution (As per Annexure-31) 6. PAN, TAN, GSTIN Certificate and any other tax related document if applicable is required to be submitted along with the eligibility bid.
2.	The bidder should be an OEM (Original Equipment Manufacturer) and/or OSD (Original Solution Developer) or their authorized Service Provider in India. In case OEM/OSD participates in the tender process directly, authorized representative will not be permitted to participate in the same tender process.	Undertaking / Power of Attorney (PoA) from the OEM/ mentioning a clause that OEM/OSD will provide support services during warranty period if the bidder authorized by them fails to perform. In case of an authorized representative, a letter of authorization from original manufacturer must be furnished in original duly signed & stamped (As Annexure-6).
3.	The bidder should have a minimum annual turnover of Rs. 100 Crore per year during the last three financial years i.e. 2022-23, 2023-24 and 2024-25. This must be the individual company turnover and not of any group of companies.	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing profit, net worth and turnover of the company for the last three financial years i.e. 2022-23, 2023-24, and 2024-25 should be submitted.
4.	Bidder should have maintained an Operating Profit in at least two financial years out of the last three Financial Years i.e. 2022-23, 2023-24 and 2024-2025	Copy of the audited balance sheet & certificate from the Chartered Accountant of the company showing Operating Profit.
5	The bidder should have Positive Net worth during the last three financial years i.e. 2022-23, 2023-24 and 2024-25.	Certificate from the Chartered Accountant for proceeding three years FY

6	The DKYC solution proposed by the Bidder should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and Work Completion Certificate or Client Reference.
7	The Bidder should have <u>experience</u> in implementing the proposed DKYC solution in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and Work Completion Certificate or Client Reference.
8	The VKYC solution <u>proposed</u> by the Bidder should have been implemented in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and Work Completion Certificate or Client Reference.
9	The Bidder should have <u>experience</u> in implementing the proposed VKYC solution in at least one or more BFSI Organization in India having minimum 500 branches.	Copy of the Purchase Order and Work Completion Certificate or Client Reference.
10	Bidder should not have been debarred / black-listed by any Bank or RBI or any other regulatory authority or Financial Institutions in India during the currency of the RFP process (till completion of RFP process).	Letter of confirmation (self-certified letter signed by authorized official of the bidder) as per Annexure-27 should be submitted
11	The Bidder should not appear in any "Caution" list of RBI / IBA or any other regulatory body for outsourcing activity as on the date of bid submission	Self-declaration to this effect on the company's letterhead should be submitted
12	Bidder under notice/termination period from OEM/OSD as on bid submission date should not bid in this tender.	Self-declaration to this effect on the company's letterhead should be submitted.
13	The service provider should ensure that there are no legal proceedings / Inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	Self-declaration to this effect on the company's letterhead should be submitted.

14	The bidder should not have: • NPA with any Bank /financial institutions in India • Any case pending or otherwise, with any organization across the globe which affects the credibility of the bidder in the opinion of Central Bank of India to service the needs of the Bank.	Self-declaration to this effect on the company's letterhead should be submitted.
15	The Bidder is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017. or The Bidder is from such a country and has been registered with the Competent Authority i.e., the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade, as stated under Annexure to the said Office Memorandum / Order and we submit the proof of registration herewith.	Certified copy of the registration certificate as per Annexure – 13 .
16	Bidder should be certified with anyone certificates among CMM Level 3 or above, ISO 27001, SOC2. (valid during the RFP process).	Supporting Document to be submitted
17	The Bidder, is not owned or controlled by any director or key officer/employee of the Bank or their relatives having the same meaning as assigned under Companies Act, 2013 and the rules framed thereunder, as amended from time to time.	Self-declaration to this effect on the company's letterhead should be submitted.

As this shall be an additional setup parallel to the existing setup, hence the incumbent vendor is not permitted to participate in the RFP process. The bidders cannot propose an incumbent solution in response to this RFP. We confirm that we are not the incumbent vendor and also confirm that we are not proposing the Bank's incumbent solution.

The bidder must submit only such documents as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same.

Bank reserves the right to verify references provided by the Bidder independently. Any decision of Bank in this regard shall be final, conclusive and binding on the bidder. Bank may accept or reject an offer without assigning any reason whatsoever.

Bidders need to ensure compliance with all the eligibility criteria points.

In case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.

In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be

considered. If an agent submits a bid on behalf of the Bidder/ OEM, the same agent shall not submit a bid on behalf of another Principal/ OEM for the same solution.

While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): Commission has decided that in all cases of procurement, the following guidelines may be followed:

In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.

If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.'

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 22: Undertaking for 5 Year Roadmap:

To,

**Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Dear Sir,

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We, _____ hereby confirm that as a bidder and the product provider, would supply, install, customize, integrate, implement, roll out, configure, maintain and support new Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels. We also commit to support the proposed Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels for a minimum period of 5 years and further period of another 2 years if extended.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 23: Compliance to Security Control:

To,

Assistant General Manager-IT
(Digital) Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Dear Sir,

Subject: Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We, _____ hereby confirm that the following security controls would be mandatorily put in place for deployment of any component of proposed Solution for Customer Onboarding through DIGITAL KYC, VIDEO KYC and other channels.

S.No	Control	Brief Description of Control Requirement
1. Physical and Logical Security		
1.1	Data center surveillance, monitoring & Physical security	Ensure that Physical security perimeters including but not limited to fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, are implemented to safeguard sensitive data and information systems. Bidder to provide complete description on implementation of plan to ensure that data center premises have defined physical access controls processes defined to segregate into various zones, this plan should include industry best practice and policies currently being followed to ensure such risks are minimized.
1.2	Background checks	Ensure background check is performed for employee/third party having direct access to systems.
1.3	Data center Environmental controls	Ensure adequate disaster protection including both natural (fire, floods etc.) and man-made (short circuit, gas leak etc.), environmental system monitoring controls are present.
1.4	Utility controls	Ensure adequate controls for supporting utilities, cabling security, equipment maintenance, and movement of assets is defined.
1.5	Data layer encryption/tokenization	Ensure procedures are established, and supporting business processes and technical measures implemented, for the use of encryption/tokenization protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations etc.), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations

1.6	Security check for an employee	Ensure that employees do not carry devices that can lead to any breach in security including but not limited to hardware devices, image capturing devices, Hazardous material etc. to avoid sensitive data breach.
-----	--------------------------------	--

2. Identity and Access Management

2.1	Multifactor authentication (MFA) for all users	MFA (one time password, bio metric authentication etc.) should be enabled for all accounts that have a console password.
2.2	User accounts Management	All credentials that have been unused in 90 or greater days should be removed or deactivated. The credentials for employees going on approved leaves should be temporarily suspended for the leave period. It is recommended that credentials for all employees who are no longer on the project team/leave the organization be permanently suspended immediately.
2.3	Root Account restriction	The "root" account has unrestricted access to all resources in the account. It is highly recommended that the use of this account be avoided. In case required, alias account to be used. Minimizing the use of this account and adopting the principle of least privilege for access management will reduce the risk of accidental changes and unintended disclosure of highly privileged credentials. Bidder to provide complete description on implementation including industry best practice and policies currently being followed to ensure all security risks arising from use of root accounts are addressed. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard
2.4	Access keys should be rotated every 90 days or less	Access keys should be rotated to ensure that data cannot be accessed with an old key which might have been lost, cracked, or stolen. Bidder to provide complete description on implementation including industry best practice and policies currently being followed to ensure all access keys are rotated at a pre-defined interval as required by the Bank. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
2.5	Password Policy/ Configuration	Bidder to provide detailed process of verification to an individual who claims it to be including industry best practice and policies currently being followed. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard. Best practices for Authentication which includes but is not limited to— • User Id to be unique • User Id must be case sensitive • User Id and password to be distinct • Password Length must not be shorter than 10 characters • Max pass length must not be too low (Max length = 128 char) • Password must be complex (Combination of alpha numeric and a special char) Or As per Bank's Policy

2.6	Maintain Current Contact details	The contact details of all employees/users with access to the System should be maintained along with a clear hierarchy. Contact details of all new users who are added to the project to be updated within a week of joining project. Periodic updating of all contact details to be carried out every quarter or as and when required by the Bank.
2.7	Security question	The cloud portal should allow account owners to establish security questions that can be used to authenticate individuals calling cloud customer service for support. It is recommended that security questions be established.

2.8	Policies Configuration and also adhere to Bank's policy	Assign Policies to either Groups or Roles to reduce the complexity of access management as the number of users grow. Policies should be the means by which privileges are granted to users, groups, or roles. It is recommended that policies are applied directly to groups and roles but not users.
2.9		Administrators should create role to allow authorized users to manage incidents.
2.10		Policies should not allow full administrative privileges and that the policies follow the principle of least privilege.
2.11		Ensure that policies minimize no. of users with full administrative privileges.
2.13	Password Policy/ Configuration	Ensure that users are notified on their primary and secondary emails on password resets. Ensure that all administrators are notified if any other administrator resets their password.
2.14	Guest users management	Do not add guest users if not needed. It is recommended to have adequate business justification and an approval workflow for guest user creation/addition. The guest user must be a separate role with view-only access

3. LOGGING AND MONITORING

3.1	Log metric filter and alarm for API calls	Real-time monitoring of API calls should be done and establishing corresponding metric filters and alarms. It is recommended that a metric filter and alarm be established for unauthorized API calls.
3.2	Log metric filter and alarm for disabling or scheduled deletion of customer created Customer Master Key (CMK)	It should be ensured that a metric filter and alarm be established for customer created CMKs which have changed state to disabled or scheduled deletion.
3.3	Log metric filter and alarm for security group changes.	Security Groups are a stateful packet filter that controls ingress and egress traffic within a VPC. Ensure that a metric filter and alarm be established changes to Security Groups.

3.4	Log metric filter and alarm for changes to network gateways.	Network gateways are required to send/receive traffic to a destination outside of a VPC. Ensure that a metric filter and alarm be established for changes to network gateways
3.5	Access monitoring across layers	Ensure adequate monitoring is done across all layers for privileged accounts

3.6	Threat monitoring	Ensure that monitoring is done at various levels including application level using tools such as IDS, IPS, DAM, SOC, SIEM & firewalls, WAF etc. The real-time report and alerts should also be shared with Bank.
3.7	Virtual environmental security	Bank's Security information and event management (SIEM) solution should be integrated with proposed solution correlate server and network logs across virtual infrastructures.
3.8	Audit Logging & Protection of logs	a) The audit logs containing confidential data must be protected. b) All audit logs consisting of user activities, exceptions and security events must be retained for forensic investigation and access control monitoring.

4. Infrastructure Security

4.1	Security groups allow access to unrestricted services.	Security groups provide stateful filtering of ingress/egress network traffic. Ensure that no security group allows unrestricted ingress access such as to port 21, 22, 80, 3389, 8080, 8888 etc.
4.2	VPC Configuration.	A VPC comes with a default security group whose initial settings deny all inbound traffic, allow all outbound traffic, and allow all traffic between instances assigned to the security group. If a security group is not specified when an instance is launched, the instance is automatically assigned to this default security group. Ensure that the default security group restrict all traffic.
4.3	Virtual environmental security	Ensure network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations should be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.
4.4	Network security	Ensure network security controls including access and authentication, intrusion detection/prevention, firewall, LBD, anti-DDOS, traffic monitoring, audit logging, technical compliance of network and controls for protection from vulnerabilities/malware/ransomware.
4.5		Network segregation of workloads shall be implemented based on the type (Production, Test, development) and purpose (user, server, interface, critical infrastructure segments etc.)
4.6		All internet traffic to the workload shall be routed through DMZ. Other network segments in the environment shall not have direct access to the internet.

4.7		Micro segmentation shall be implemented
4.8	Virtual environmental security	Ensure each operating system are hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standards or default template. This shall be reviewed annually.
4.9	Encryption & Key management	Sensitive data fields need to be protected using encryption/hashing/tokenization as appropriate.

4.10	Key management	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall be stored on Bank provided Key management Solution. Key management and key usage shall be separate duties.
------	----------------	---

5. Application and Process Security

5.1	Application Security : API security	Application programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, and regulatory compliance obligations.
5.2	Application Security: Access Control	Improper access control, such as improper direct object references, failure to restrict URL access, & directory traversal must be stopped by properly authenticating users & sanitizing input. Also, internal object references must not be exposed to users. Such controls to be incorporated for vulnerabilities such as insecure ids, path traversal etc.
5.3	Application Security: Cross Site Scripting (XSS) Flaws	Bidder to provide complete description on implementation including industry best practices and policies currently being followed to ensure application cross-site scripting flaws are addressed. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
5.4	Application Security: Denial of Service	Bidder to provide complete description on implementation including industry best practices and policies that are being followed. Ensure that anti-DDoS tool should be implemented. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
5.5	Application Security: Injection Flaws	Bidder to provide complete description on implementation including industry best practices and policies currently being followed to ensure injection flaws are addressed. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
5.6	Application Security: Authentication and Authorization for Web services	Allows messages to include credentials to aid receivers in determining whether or not the message sender is authorized to perform the requested action. Bidder to provide complete description on implementation including industry best practices and policies currently being followed to ensure authentication and authorization for web services. Description should include implementation of tokens such as SAML assertion, ISO Rights Expression Language, IETF Kerberos Token, username/password etc. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.

5.7	Application Security: Access Across interfaces	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.
5.8	Application Security: Authentication	Authentication parameters should include following: Password Strength, communication, password change, Failed login, Session timeout, Dormancy and blocking on multiple failed attempts to authenticate
5.9	Application Security : Role matrix	Ensure that Role based authorization mechanism must be used for allocating privileges to the users. The application must have the provision to define different levels of users or roles. The roles must have segregation of duties such that an individual must not be responsible for more than one of the following duties: business, data entry, computer operation, network management, system administration, systems development, change management, security
		administration and security audit. The security matrix must be automatically generated by the application and available for review at least once in every quarter or as and when required.
5.10	Application Security: Session time out	Ensure that the Inactive sessions must shut down after a defined period of inactivity. This must be a parameter setting.
5.11	Application Security: Validation of session identifiers	Ensure that the Session identifiers must be validated at the time of every request by the server to verify that the requesting user is an authenticated user.
5.12	Application Security: Role based Security Matrix	Ensure that Role based authorization mechanism must be used for allocating privileges to the users. The application must have the provision to define different levels of users or roles. The roles must have segregation of duties such that an individual must not be responsible for more than one of the following duties: business, data entry, computer operation, network management, system administration, systems development, change management, security administration, security audit. The security matrix must be automatically generated by the application and available for review at least once in every quarter or as and when required.
5.13	Process security	Ensure that files are scanned for data format, size, unwanted malicious code etc., before uploading it or using it for any purpose. Files must be validated for allowable extensions. Dangerous extensions like .js, .exe, .html, etc. must be banned.
5.14		Ensure change management process is defined for processes like patching of systems, application patches, system upgrades etc. It is pertinent that documentation of all such changes is maintained in detail along with impact analysis for the entire contract period.
5.15	Support for Multi-tenancy and related security features	If the application is deployed on the Cloud using native multi-tenancy features offered by the application, privacy of data across tenants or entities needs to be ensured through appropriate access control mechanisms.

5.16	Application Security: Scanning of files before uploading	Ensure Files are scanned for data format, size, unwanted malicious code, which may lead to cross site scripting attack, where possible, before uploading it or using it for any purpose. Files must be validated for allowable extensions. Dangerous extensions like .js, .exe, .html, etc. must be banned.
6. Cyber Security, Governance and Compliance		
6.1	Migration of data	Ensure that data imported on Bidder application is done in a consistent manner to maintain integrity of the data. The error logs pertaining to the pre-migration, migration and post migration period shall be available Data migration reports to be prepared and shared with the Bank as and when data migration is performed by the Bidder.
6.2	Migration to new system	In case of migration to new system at Bidder end, ensure that complete transaction data and audit trails from the old system to the new system shall be migrated Data migration reports to new system to be prepared and shared with the Bank as and when data migration is performed by the Bidder.
6.3	Data privacy	There shall be proper access control to view and download the data by authorized users. The Bidder must come up with an actual, specific, independent security standard that is updated and audited quarterly or at a frequency as defined by the Bank. In addition, for sensitive data like Personally Identifiable Information (PII), Aadhaar etc., the specific Security, regulatory, statutory, and legal requirements shall be applicable. Regular audits at a pre-defined frequency should be conducted by the Bidder with the Bank having access to the audit results.
6.4	Data leakage	There shall be adequate data leakage prevention tools deployed on entirety of the data as and when shared by the Bank or its customers. For e.g., In case of Platform as a Service or Infrastructure as a Service, Bank may load test data on the solution provided If this represents a subset of the live data, it needs to be protected e.g. sensitive elements like customer ID, name, address, phone number, account number, need to be tokenized/hashed so that the risk of data leakage is minimized. The bidder and the Bank need to agree on the sensitive elements that need to be tokenized/hashed. Bidder to provide complete description on implementation of data leakage tools including industry best practices and policies currently being followed to ensure such risks are minimized. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
6.5	Data Segregation And Isolation	Ensure that sufficient controls are in place to maintain confidentiality and integrity of data. Bidder to provide complete description on implementation of data segregation and isolation tools including industry best practices and policies currently being followed to ensure such risks are minimized. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.
6.6	Data Sovereignty	Ensure that all regulatory compliances are taken into consideration for data sovereignty related to all bank and customer data. Bidder to provide complete description on implementation including industry best practices and policies currently being followed to ensure such risks are minimized. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard.

6.7	Vulnerability Management	Maintain a vulnerability management program and ensure that network and applications are scanned on a pre-defined frequency as decided by the Bank. Bidder to have a vulnerability remediation process in place with provisions for carrying external vulnerability assessment. Vulnerability management reports to be prepared and shared with the Bank as and when at a pre-defined frequency.
6.8	Data Disposal	Data disposal processes to delete data from a system that is no longer needed and required by law or policy to be retained (on defined frequency in a secure manner). Bidder to provide complete description on implementation of data disposal processes including industry best practices and policies currently being followed to ensure such risks are minimized. Additionally, compliance to all regulatory, statutory and legal guidelines to be followed in this regard. Further, Bidder to provide certificate signaling successful disposal of data as and when data disposal processes are conducted.
6.9	Access to data	Bank to have access to all customer and bank data for Purposes of Discovery, Emergency Security Issues, Disclaimer of Warranty, Indemnification, Guarantees and metric, Service Usage, Service Activation, Governing Law and Jurisdiction and right to Audit, or any other purposes if so required by the Bank.

6.10	Adherence To regulatory compliance	The Bidder to ensure compliance to RBI's IT Outsourcing Policy, IT Act, ISO 27001, ISO 22301, ISO 27701, SOC 2 Type II, CSA Star Level 2 Adherence to at least Level 3 of process capability levels under the COBIT 5 Process Assessment Model based on ISO 15504-2, and to all applicable RBI guidelines and circulars for managing service agreements, risk, security, privacy, data manage and storage continuity and compliance (as agreed). Bidder to ensure compliance to all applicable ISO, RBI and other statutory, regulatory and legal guidelines as and when in forced by the respective authorities.
6.11	Testing of plan	Business continuity, security incident Response, software/ application/ system upgradation, data migration on end of contract plans shall be subject to testing at planned intervals, upon significant organizational or environmental changes or as and when required by the Bank. Incident response plans shall involve but not be limited to impacted customers (tenant) and other business relationships that represent critical intra-scope chain business process dependencies. Reports on plans for business continuity and incident response to be prepared and shared with the Bank as and when at a pre-defined frequency.
6.12	Policy & process for BCP & DR drill	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel. Periodic review of all policies and procedures and conducting of BCP and DR drill to be conducted quarterly or at a frequency as defined by the Bank.

7. Other requirements

7.1	Regulatory, Statutory and legal requirement	Bidder to comply with all applicable Regulatory, Statutory and legal requirements which are in effect currently, or future requirements as and when enforced by the respective authorities. Further, Bidder to comply with all bank policies pertaining to ISMS, Data security, data privacy, data storage etc. which are in effect currently, or future requirements as and when enforced by the Bank.
7.2	Audit requirements	Bidder to comply with both internal and external audits as conducted by the Bank or bank appointed agency of all policies, procedures, plans etc. quarterly or at a frequency as defined by the Bank.

7.3	Migration of data on termination of contract	Bidder to provide detailed plan for migration of all bank and customer data which will include but not be limited to data structures, data dictionary and meta data on termination of contract. Further, Bidder to conduct periodic review of the plans on planned intervals, upon significant organizational or environmental changes or as and when required by the Bank. On discontinuation of contract, all bank and customer data should be provided back to Bank. In such case, Bidder should also provide all required support to handhold the solution and data to new ISV.
-----	--	---

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 24: Undertaking for Information Security:

(This letter should be on the letterhead of the bidder duly signed by an authorized signatory on Information security as per regulatory requirement)

To,

**Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Subject: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).

Also, undertake that the proposed solution / software to be supplied will be complying to Bank's Information Security Policy (of the version of the application being delivered as well as any subsequent versions/modifications done). And new Information Security requirement will be compiled within the timeline set by Bank / Regulatory agencies.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 25: Undertaking for Data Privacy:

(This letter should be on the letterhead of the bidder duly signed by an authorized signatory on Data Privacy requirement)

To,

**Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sir,

Subject: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

We hereby undertake to comply with the regulations of Digital Personal Data Protection Bill (DPDPB 2023) and any future amendment/addition to the Bill in future as part of the engagement during entire period of contract.

Further, we ensure that the Data privacy, security and confidentiality of the Bank shall not be compromised.

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 26: Format for Local Content : (Make in India)

(This letter should be on the letterhead of the bidder as well as the OEM/ Manufacturer duly signed by an authorized signatory on Information security as per regulatory requirement)

CERTIFICATION FOR LOCAL CONTENT

To,

**Assistant General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614**

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Bidder Name:

This is to certify that the "RFP for Procurement, Implementation and Maintenance of Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels" is having the local content of ___% as defined in the above-mentioned RFP and amendment thereto.

This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 – Revision vide Order No. P-45021/2/2017-PP (BE-II) dated 04th June 2020.

Signature of Statutory Auditor/Cost Auditor

Registration Number:

Seal:

Countersigned by the bidder:

Bidder – (Authorized Signatory)

Date:

Place:

Annexure 27: Undertaking for Non- Blacklisting/ Non-Debarment of the bidder

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

- 1) I/We, Proprietor/Partner(s)/Director(s) of M/s.....hereby confirm that I/We have read and understood the eligibility criteria and fulfil the same.
- 2) I/We further confirm that all the information furnished by me/us, as per the requirement of the Bank, have been included in our bid.
- 3) I/We further hereby undertake and agree to abide by all terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our bid.
- 4) I/We further hereby undertake and agree to bring to the notice of the Bank in case of blacklisting / debarment if any during the RFP process.
- 5) *I/We further hereby declare that I/We have not been black-listed or otherwise debarred by any Bank/Financial Institution/Central Government/ State Government/any Central or State Undertaking or Corporation/ Reserve Bank of India or any other Regulatory Authority or any other Statutory Authority as on date of the publication of this Tender/Procurement.

(OR)

I/We further hereby declare that the Proprietorship Concern/Partnership Firm/Company/..... (if any other entity) namely M/s was blacklisted/debarred by(Name of the Authority who blacklisted/debarred) from taking part in their Tender/Procurement for a period ofyears w.e.f.to..... The period is subsisting/over on.....and now I/We is/are entitled to take part in Tender/Procurement.

- 6) I/We declare that no proceedings/inquiries/investigations have commenced/pending against me/us by any Statutory Authority/Regulatory Agency/Investigating Agency which may result in liquidation of company/ firm/proprietorship concern and/or may act as deterrent on the continuity of business and/or may hamper in providing the said services, as envisaged in this document.

- 7) I/We further hereby declare that no legal action is pending against me/us for any cause in any legal jurisdiction.
- 8) I/We undertake that adequate number of resources, if required by the Bank, will be deployed for the project to complete the assignment within the stipulated time.

***STRIKE OUT WHICH IS INAPPLICABLE**

(Deviation to the above if any, the Bidder must provide details of such action(s))

Signature of Authorized Signatory:

Name of Signatory:

Designation:

Seal of Company:

Date:

Place:

Annexure 28: Masked Commercial Bid

To,

Asst. General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

All the costs are to be mentioned in Indian Rupees including GST.

TCO Summary Table									
Sr. No#	Category	Year 1	Year 2	Year 3	Year 4	Year 5	Total Cost	GST	Total Cost with GST
1	Table A: Application License Costs(Including DC&DR)	XXXX					XXXX	XXXX	XXXX
2	Table B: Third Party Software License Cost	XXXX					XXXX	XXXX	XXXX
3	Table C: Implementation Cost	XXXX					XXXX	XXXX	XXXX
4	Table D: Training Cost	XXXX					XXXX	XXXX	XXXX
5	Table E: Annual Technical Support (ATS)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
6	Table F: Facility Management Cost	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
7	Table G: User Defined Customization (Change Requests)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
8	Table H: Any Other components	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
	Total Yearly Cost	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
	Total Cost to Ownership TCO								XXXX
	TCO in words	XXXXXXXXXXXXXXXXXXXX							

Table A: Application License Costs

SR. NO	Item Description	Unit Cost	Cost	GST	Total Cost with GST
1	Enterprise License cost of VIDEO KYC Solution (Including DC and DR)	XXXX	XXXX	XXXX	XXXX
2	Enterprise License cost of DIGITAL KYC Solution (Including DC and DR)	XXXX	XXXX	XXXX	XXXX
	Total (A)	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table B: Third Party Software License Cost

SR. NO	Item Description	Details of Software	No of Units(P)	Unit Cost (Q)	Cost R = (P) x (Q)	GST	Total Cost with GST
1	Operating System (OS). (If OS proposed by vendor is RHEL on S390X no cost is to be mentioned)			XXXX	XXXX	XXXX	XXXX
2	Database License. (If Database proposed by vendor is Oracle 19C and above, no cost is to be mentioned) However units to be mentioned			XXXX	XXXX	XXXX	XXXX
3	Middleware other than WebLogic (if any give details)			XXXX	XXXX	XXXX	XXXX
4	Third Party Utilities – 1 (if any give details)			XXXX	XXXX	XXXX	XXXX
5	Third Party Utilities – 2 (if any give details)			XXXX	XXXX	XXXX	XXXX
6	Third Party Utilities – 3 (if any give details)			XXXX	XXXX	XXXX	XXXX
7	Third Party Utilities – 4(if any give details)			XXXX	XXXX	XXXX	XXXX
	SUB TOTAL (B)			XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table C: Implementation Cost

SR.NO	Item Description	Number of Journeys [A]	Rate per Journey [B]	Cost [A X B]	GST	Total Cost with GST
1	VIDEO KYC JOURNEYS	15	XXXX	XXXX	XXXX	XXXX
2	DIGITAL KYC JOURNEYS	15	XXXX	XXXX	XXXX	XXXX
	SUB TOTAL (C)	30	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table D: Training Cost

SR.NO	Item Description	Unit Cost	Cost	GST	Total Cost with GST
1	Training Cost	XXXX	XXXX	XXXX	XXXX
	Total	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table E: Annual Technical Support (ATS)									
Sr. No#	Annual Technical Support (ATS)	Details of the Software	Year-2	Year-3	Year-4	Year-5	Total Cost	GST	Total Cost with GST
1	ATS of VIDEO KYC (ATS for a period of 4 years after completion of one year warranty)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
2	ATS of DIGITAL KYC (ATS for a period of 4 years after completion of one year warranty)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
3	ATS of OS if other than RHEL on S390X (ATS for a period of 4 years after completion of one year warranty)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
4	ATS of Database if other than Oracle (ATS for a period of 4 years after completion of one year warranty)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
5	ATS of any Middleware other than WebLogic (ATS for a period of 4 years after completion of one year warranty)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
6	Third Party Utilities – 1 (if any give details)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
7	Third Party Utilities – 2 (if any give details)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
8	Third Party Utilities – 3 (if any give details)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
9	Third Party Utilities – 4(if any give details)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
	SUB TOTAL (E)		XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table F: Facility Management Cost										
Sr. No#	Facility Management Cost	No of resources	Year- 1	Year-2	Year- 3	Year- 4	Year- 5	Total Cost	GST	Total Cost with GST
1	Dedicated Support Charges of onsite L2 resources for a period of five years post Go- Live (Number of resources X Per Month Cost X 12 Months)	4	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
2	Support Charges of onsite Database Administrator (DBA) for a period of five years post Go- Live (Number of resources X Per Month Cost X 12 Months)	1	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
3	Support Charges of Onsite Development team (Frontend & Backend or Full-stack) for a period of five years (Number of resources X Per Month Cost X 12 Months)	3	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
	SUB TOTAL (F)	8	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table G: User Defined Customization (Change Requests)									
Sr. No#	User Defined Customization (Change Requests)	Year- 1	Year-2	Year- 3	Year- 4	Year- 5	Total Cost	GST	Total Cost with GST
1	Cost for 50 Man days per year for the TCO purpose, payment will be made as per FPA method for actual expenses for Change Request. Amount to be quoted is (50 X man day rate per year). (Number of resources X Per Month Cost X 12 Months)	N/A	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX
	SUB TOTAL (G)	N/A	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX

All amounts in the Bill of Material should be in INR

Table H: Any other Components

SR.NO	Item Description	Details of Components	No of Units(P)	Unit Cost(Q)	Cost R = (P) x (Q)	Year 1	Year 2	Year 3	Year 4	Year 5	GST	Total Cost with GST
	Any other Component 1			XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
	Any other Component 2			XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
				XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
	Total			XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX

All amounts in the Bill of Material should be in INR

Notes:

- 1) The price arrived / discovered through RFP will be valid for the contract period of 5 years.
- 2) All licenses including third party Licenses related to this System should be in the name of Bank. However, Bank is providing database licenses of Oracle 19C and above, RHEL on S390X if required, but bidder should arrange support for Oracle Database and OS, Middleware.
- 3) Bidder should apply the patches as well as security updates and implement Bank's Base line security as per Bank's IT security policy for all the infra & DB components.
- 4) All the related Software such as operating system, Java, Apache Tomcat, Search engine etc., if any, must be included in above commercials. Bank will not allow any additional commercials for these. If anything missed and required for all above Solutions. It will be the responsibility of Bidder to provide the same at no additional cost to the Bank.
- 5) In case of any discrepancy in TCO amount, the figure in words will be treated as final.
- 6) The ATS charges per annum should be minimum 15% of the License cost of software components.

- 7) Facility Management Cost (Unit Price of dedicated support) is for entire project period of five (5) years. Bank has the option to avail onsite support on same rate if needed extra onsite resources in due course of time during the contract period of five (5) years. Bank has also option to reduce the number of onsite resources if needed during contract period of five (5) years.
- 8) Quantity mentioned here is only indicative for deriving TCO. Actual quantity may increase or decrease as per requirement.
- 9) All the changes sought by Regulatory and Statutory authorities received from time to time during contract period and subsequent renewals, if any, must be carried out at no extra cost to the Bank.
- 10) Any unused man days in a year under the head "**User Defined Customization (Change Requests)**" shall be carried forward to the subsequent year within the same rate.
- 11) Selected bidder should integrate all the components Web, App, DB, etc. with the bank provided Application Performance Monitoring (APM) tool at no extra cost.
- 12) The bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP and the corrigendum in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully utilize the solution.
- 13) Bank will not be responsible for any arithmetic errors in the commercial bid details sheet committed by the bidders. All formulas & arithmetical calculations will be Vendor's responsibility.
- 14) The bidder is expected to specify the type of licenses along with the details with respect to quantity, rate, etc., wherever applicable.
- 15) In case the bidder includes/combines any line item as part of any other line item in the commercial bid, then this has to be clearly mentioned in the description indicating the line item which contains the combination
- 16) The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
- 17) The Bidder may insert additional line items as applicable based on the solution offered in the respective tabs
- 18) The Bidders should quote as per the format of Bill of Material ONLY and a masked replica of the Bill of Material should be enclosed in the technical bid.
- 19) Bidder is required to cover component by component licensing details for each of the software components proposed to CBI
- 20) The masked Bill of Materials which would be submitted as part of the Technical Bill of Material should contain "XXXX" for ALL the corresponding commercial values that will be present in the unmasked Bill of Material that will be part of the Commercial submission.
- 21) All amounts in the Bill of Material should be in INR
- 22) The Bidder should to the extent possible stick to the same structure of the Bill of Material. Hence, the bidder is not expected to delete necessary rows.
- 23) Any additional items (software, hardware) and services to be procured by the Bank in

the future shall be priced on a pro-rata basis, based on the rates specified in the Bill of Material, unless otherwise determined by the Bank at its sole discretion. The Bidder is required to comply with this provision.

- 24) If the Bidder has not provided a specific quote for any line item listed in the Bill of Material, it shall be deemed that the Bidder has included the cost for such an item within the overall pricing provided in the Bill of Material. No additional charges beyond those specified in the Bill of Material will be payable by the Bank.
- 25) Bidder is required to submit the commercials during the bid submission and is required to provide the line item wise detailed breakup in the commercial bid.
- 26) Bidder shall comply to the Installation & commissioning, implementation scope provided in the RFP
- 27) Bidder should quote for end-to-end Installation & commissioning, implementation scope as mentioned in the RFP
- 28) Activities and functions to be undertaken for installation and implementation of the licensed software should be as per the RFP.
- 29) Bidder is expected to provide a detailed break up of all products and services that are under the scope as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management.
- 30) The ATS costs for Production DC & DR have to be quoted separately
- 31) If required, the Bidder has to create additional line items in this section.
- 32) ATS should be quoted minimum 15% of Software Costs
- 33) Bidder is expected to quote for each calendar year
- 34) For any additional person-days above the 50 person-days, the rate quoted for that year will be considered. i.e. For any additional requirement of person-days and bidder should not make any additions/increase to the yearly rate/charges of the person-days.
- 35) Bidder is expected to fill all the values of the BOM, if any item doesn't pertain to the bidder numeric value zero to be filled. If any cell is missed or blank the application will be considered as incomplete and Bidder will be debarred from bidding process.
- 36) Bidder to carry forward the unutilized person-days (with same quoted cost) to the subsequent years. No additional cost to be charged to Bank

Authorized Signatory: _____

Name & Designation & mail id: _____

Business Address: _____

Date:

Place:

Annexure 29: Functional Specifications

The bidders should provide their response against each of the Functional Specifications as per the details mentioned in the table below. Functional Specifications which are not available should be customized as per Bank’s requirement without any additional cost.

Availability of the feature	Marks per feature
Available (YES)	1
Not Available (NO)	0

Module	No of Requirements
VIDEO KYC (VCIP)	78
DIGITAL KYC	64
Total	142

The Above Marks shall be normalized to 50 using the formula below:

$$\text{Normalized Marks} = \frac{\text{Marks Scored}}{\text{Total Marks}} \times 50$$

No.	VIDEO KYC (VCIP)		
Sr No.	Functional Requirements	Available (YES / NO)	Remarks
1.	The VKYC Solution should be able to be integrate with Bank's existing and upcoming applications to perform VKYC.		
2.	Video-KYC Solution must comply all the functional and technical requirements as per latest RBI circular/guidelines and advisories as and when released by the regulator and any amendments thereof in future.		
3.	Application should support single login for agent/auditor to perform and review the VKYC irrespective of business journeys. Two Factor Authentication (2FA) is also required for bank user login		
4.	Application should allow customers to verify their identity through video interaction as per RBI Guidelines. This may involve capturing images of government-issued identification documents such as Aadhaar card, PAN Card, etc., extraction of Data through OCR and comparing the same with the KYC documents submitted by the customer. Documents and captured images /data should be available at both agent/auditor/admin login.		
5.	The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy. Appropriate artificial intelligence (AI) technology should be used to ensure that the V-CIP is robust.		
6.	System should have functionality of challenge-Response method as part of the questionnaire during VCIP process. Agents will verify the identity of customers based on the common random questions majorly in all journeys with respect to KYC of customer. Application should also have the functionality of configurable Random Security questions if required for a particular journey through admin portal /API and same will be verified by agents for that specific journey only.		

7.	The application should Capture Photograph of the customer and able to calculate the face match score with the latest photo taken by the agent with the images passed to VKYC solution to ensure a high degree of Facial match percentage with low false positive and high accuracy similar to verify the customer's identity during the video call. Application should also have the facility to define threshold of the face match score to suggest agents to accept or reject. The solution should also perform face match with multiple images passed to VKYC solution like CKYCR image, Aadhaar image, PAN image etc.		
8.	Live Geo-tagging, VPN detection & IP capture while performing V-CIP. Application should be able to alert and halt the V-CIP process if the location is not in India. Solution should be able to detect spoofing and cross verify the location of IP Address and through Latitude and longitude captured through web browser.		
9.	Solution should Record (both video & audio) LIVE VCIP process with the customer. The quality of the video recording should be adequate to identify the customer beyond doubt.		
10.	Provision to capture signature of the customer through the proposed solution.		
11.	Application should be able to do end-to-end encryption (data at rest, data in transit) of data between customer device and the hosting point of the V-CIP application as per appropriate encryption standards. Data should be stored in encrypted form especially PII Data of customer.		
12.	The customer consent should be recorded in an auditable and alteration proof manner.		
13.	Application should be able to encrypt communication of traffic from Bank Applications/platform to VKYC application using latest TLS/SSL		
14.	Application should be capable of integrating with bank's internal systems/platform such as Active directory (AD), CBS, CKYCR application, email gateway, SMS gateway etc. for data fetching, reverse updating, processing etc. Further, also able to integrate with Bank's other security solutions.		
15.	Application should be horizontal and vertical scalable to meet any incremental requirement		

16.	Queuing mechanism and the approximate wait time, etc. to be made available to the customers. Efficient management of customer queues to ensure timely assistance and reduce wait times. This may include features such as virtual queue management, estimated wait time display, and prioritization based on urgency or type of service.		
17.	Application should distribute Video calls among available agents based on factors like language, location, availability of agents, time and ad hoc basis to particular agent. Automated routing algorithms can ensure fair distribution and optimal utilization of resources.		
18.	The solution should support multilingual platform and should ask customer for their preferred language and show further instructions in his/her preferred language.		
19.	Solution should have provision to select initiate call now/ schedule call. Option should be available for the customer to schedule a future slot for V-CIP and to initiate V-CIP call to complete the process then and there.		
20.	Solution should have capability to complete VKYC process even on low bandwidth on customer end.		
21.	Solution should provide network connection quality indicator for both end (VKYC Agent & Customer)		
22.	Provision for maker /checker/ auditor role to any office/ unit shall be provided.		
23.	Provision to reschedule and/ or rebook an appointment, cancel the booked slot by the customer/ back-office personnel of the bank should be available.		
24.	Leave marking/holiday marking/non-working hour marking provision should be available for all the Users in admin portal. Customer should not able to book appointment for non-working hours. Leave management module in the Admin portal must have provision to re-assign/reallocate/ cancel the booked calls to other agents or dynamic allocation to other agents if any agent is on leave/unable to make call.		
25.	The solution has built-in Document Management System to store all the documents and images captured and downloaded in the VCIP process.		

26.	Video session should be capable to recognize the face and should not allow capturing the picture of user if the face is not recognized in the frame/by AI tools. Client-side session should not be started until all requirements for video session are met like adequate lighting, adequate network speed, permissions like camera, Microphone, Geo-location etc.		
27.	Session Management: In case of disruption of any sort including pausing of video, reconnecting calls etc. should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, there is no need to initiate a fresh session. However, in case of drop/disconnection, fresh session shall be initiated.		
28.	Provision for in-built chat (text-based) in case of any assistance to be given to the customer. Chats should be logged.		
29.	System should display all the data regarding face matching score, Document verification for forgery, liveness check, geo-location, etc. as a dashboard for the application so that agent/auditor can view them in one place before approving or rejecting. A scoring on all the metrics to be provided. An executive dashboard for agents and admin users to monitor ongoing video calls, queue status, wait times, agent performance and overall system health.		
30.	Agent/auditor should be able to provide additional remarks and either mark as ACCEPTED/ REJECTED/ SUSPICIOUS with reasons.		
31.	Agent/Auditor level rejection option to be made available with the pre-defined reason list as provided by the Bank and the list of reasons should be configurable by Bank		
32.	Solution should provide detail MIS reporting related to system monitoring and business monitoring at each hierarchical level viz BRANCH/RO/ZO/CO. Search option should be available to know the status of a particular application or unique ID.		
33.	Application vendor ensure the database optimization like creation of Indexes, optimizing DB queries etc. to maintain the smooth functioning of application.		

34.	eDocument verification including Aadhaar, PAN card, Passport, Voter ID, Driving License, NREGA card and any other OVD through integrations with the corresponding systems as per regulatory/statutory guidelines.		
35.	Provision to integrate with Digi Locker to access customer KYC Documents.		
36.	The solution should be able to generate the VCIP report from the VCIP process and able to send as an e-mail attachment to the branch concerned. The report should contain the customer information, photograph captured during the call, OVD images and the details of agents, approver, and auditor with remarks.		
37.	The solution should have Role based access for all users such as Branch/ Admin/ Auditors/ Agents etc.		
38.	All the activity log along with the credentials of the official performing the V-CIP shall be preserved.		
39.	All the recordings should also be tagged with reference number and the date and timestamp of the recordings. The video recordings should contain live GPS co-ordinates and date-time stamp as per the RBI guidelines.		
40.	Recordings should be available to auditors on immediate (near real time basis within minimum time) to review the conversation as per RBI guidelines / SOP of the Product.		
41.	Recordings should be able to easily exported as and when required for compliance purposes in standard format MP4, AVI etc., Admin portal to search based on unique identifier and further able to download as per approved video formats.		
42.	Solution must support the capability to redact or black out the Aadhaar Number/Other PII in the stored video. Solution should mask the PII while displaying in DB and Video Recording.		
43.	Develop any custom MIS reports as per the requirement of our Bank with various filters.		

44.	The software should have real-time analytics of various metrics such as: Agent Rejections & Acceptance Audit rejections & Acceptance Pending at Auditor level Schedules Pending		
45.	The reports generated should be downloadable / exportable in Human readable format like Excel, pdf, csv, text etc.		
46.	Internal Dashboard to admin users for API status: Internal web portal is required for admin users which provide information for each application related to API audit logs for each API like API request, Response, status of API failure /success.		
47.	The solution should be compliant with all latest guideline of the regulatory authorities. During the contract period, successful vendor needs to make necessary changes in the solution to meet regulatory requirement changes at no additional cost to the Bank.		
48.	The bidder should ensure that all the regulations of Information Technology Act, 2000 as amended from time to time, are being adhered to.		
49.	Regular compliance of audit points raised/observed during internal audits and external audits of the application without any additional cost to the Bank within the prescribed timelines decided by the Bank.		
50.	The solution must undergo software and security audit (code audit by CERT-in empaneled auditor, RBI and any other regulators, VAPT audit in the bank end, etc.) as per stipulations and all remarks / observations in the audit reports to be rectified / incorporated.		
51.	Bank reserves right to conduct audits on the system provided by the bidder. Bidder to provide necessary arrangement and access control for the Bank.		
52.	Bidder should maintain and support its software and subsequent updates, upgrades and bug fixes such that the software remains updated and secured from vulnerabilities.		

53.	The solution should be device compatible and platform agnostic. Responsive web pages for friendly display in mobile devices/TAB		
54.	Security events, audit trails for all events and logs should be available for administrators and user activity should be enabled to monitor and detect suspicious activity.		
55.	The system shall maintain a log of failed and successful attempts to logon to the system.		
56.	Should comply with data retention and destruction schedules/ Policy provided by Bank.		
57.	Perform regular backup and recovery tests.		
58.	To provide Forensic Investigation Support as and when required by the Bank.		
59.	Application should restrict upload to specific types of files extensions, file size and content type.		
60.	Application should demonstrate sufficient protection against redirection flaws. Application should protect against click jacking.		
61.	Robust data backup, recovery and storability procedures with offsite and onsite backup		
62.	Application makes use of available security protocols (e.g. HTTPS, SFTP/FTPS, LDAPS, SSH, etc.) to protect sensitive data during transmission over private and public networks.		
63.	Application uses encryption (or equivalent controls such as hashing) to ensure the confidentiality and integrity of user password in storage. This involves usage of encryption technologies that have been thoroughly and publicly tested (e.g. 128-bit key length for symmetric encryption).		
64.	The Solution should be deployable on Cloud native architecture with the adaptability to the on demand up-scaling and down-scaling and seamless failover movements of the instances.		
65.	The system should have proper business continuity plan. As part of BCP, the system should be implemented at Bank's data center and disaster recovery center.		

66.	The solution should be available on High availability at DC and DR.		
67.	The bidder should provide training on performing V-CIP for selected officials. A detailed curriculum should be planned for this training program in consultation with Bank.		
68.	On the job training shall be given for Bank Officials of the Bank at Bank's Premises.		
69.	Analyzing the location details captured during the V-CIP process to identify large number of opening of accounts in locations with very near proximity In a SUSPICIOUS manner and give a warning to the V-CIP Official.		
70.	Should support compression of data with precaution that quality of Video and data should not be deteriorate and decompressed after storing at Bank end if required to facilitate faster data transfer.		
71.	The application should lock the session after a specified number of authentication failures.		
72.	Provide ability for administrators to archive and backup content using one Web-based user interface.		
73.	User names and passwords must be hashed or encrypted at storage as well as before passing them over the network for authentication purpose. Hashing should confirm to at least SHA256 and above + Salt		
74.	Should support at least AES 256-bit encryption and above between web browser & web server front end (Internet & Intranet)		
75.	Proposed system should be able to disable the copy/paste and screen capture capabilities		
76.	Solution and Exposed APIs must adhere to Information Security (IS) requirement/policy of the bank/RBI's security requirements.		
77.	Solution must adhere to Data localization norms and privacy protection norms as per our bank's Statutory and Regulatory requirements		
78.	The proposed Video KYC application should be compatible with and functional on the Hardware infrastructure and Operating System provided by Bank.		

No.	DIGITAL KYC (DKYC)		
Sr No.	Functional Requirements	Available (YES / NO)	Remarks
1.	The DKYC Solution should be able to be integrate with Bank's existing and upcoming applications to perform VKYC.		
2.	DKYC Solution must comply all the functional and technical requirements as per latest RBI KYC Master directions, circular/guidelines and advisories as and when released by the regulator and any amendments thereof in future.		
3.	Application should support single login for agent/auditor to perform and review the DKYC irrespective of business journeys. Two Factor Authentication (2FA) is also required for bank user login		
4.	Application should allow customers to verify their identity through in-person interaction as per RBI Guidelines. This may involve capturing of biometrics and images of government-issued identification documents such as Aadhaar card, PAN Card, etc., extraction of Data through OCR and comparing the same with the KYC documents submitted by the customer. Documents and captured images /data should be available at both agent/auditor/admin login.		
5.	The application shall have components with face liveness detection as well as face matching technology with high degree of accuracy. Appropriate artificial intelligence (AI) technology should be used to ensure that the process is robust.		
6.	The application should Capture Photograph of the customer and able to calculate the face match score with the latest photo taken by the agent with the images passed to DKYC solution to ensure a high degree of Facial match percentage with low false positive and high accuracy similar to verify the customer's identity. Application should also have the facility to define threshold of the face match score to suggest agents to		

	accept or reject. The solution should also perform face match with multiple images collected from CKYCR image, Aadhaar image, PAN image etc.		
7.	Live Geo-tagging while capturing the photos.		
8.	Provision to capture signature of the customer through the proposed solution.		
9.	Application should be able to do end-to-end encryption (data at rest, data in transit) of data between the device and the hosting point of the application as per appropriate encryption standards. Data should be stored in encrypted form especially PII Data of customer.		
10.	Application should be able to encrypt communication of traffic from Bank Applications/platform to DKYC application using latest TLS/SSL		
11.	Application should be capable of integrating with bank's internal systems/platform such as Active directory (AD), CBS, CKYCR application, email gateway, SMS gateway etc. for data fetching, reverse updating, processing etc. Further, also able to integrate with Bank's other security solutions.		
12.	Application should be horizontal and vertical scalable to meet any incremental requirement		
13.	The solution should be multilingual		
14.	Solution should have capability to complete KYC process even on low network bandwidth.		
15.	Solution should provide network connection quality indicator on TAB		
16.	Provision for maker /checker/ auditor role to any office/ unit shall be provided.		
17.	Leave marking/holiday marking/non-working hour marking provision should be available for all the Users in admin portal.		

18.	The solution have built-in Document Management System to store all the documents and images captured and downloaded in the on-boarding process.		
19.	System should display all the data regarding face matching score, Document verification for forgery, liveness check, geo-location, etc. as a dashboard for the application so that agent/auditor can view them in one place before approving or rejecting. A scoring on all the metrics to be provided. An executive dashboard for agents and admin users to monitor ongoing sessions, queue status, agent performance and overall system health.		
20.	Agent/auditor should be able to provide additional remarks and either mark as ACCEPTED/ REJECTED/ SUSPICIOUS with reasons.		
21.	Agent/Auditor level rejection option to be made available with the pre-defined reason list as provided by the Bank and the list of reasons should be configurable by Bank		
22.	Solution should provide detail MIS reporting related to system monitoring and business monitoring at each hierarchal level viz BRANCH/RO/ZO/CO. Search option should be available to know the status of a particular application or unique ID.		
23.	Application vendor should ensure that the database optimization like creation of Indexes, optimizing DB queries etc. to maintain the smooth functioning of application.		
24.	eDocument verification including Aadhaar, PAN card, Passport, Voter ID, Driving License, NREGA card and any other OVD through integrations with the corresponding systems as per regulatory/statutory guidelines.		
25.	Provision to integrate with Digi Locker to access customer KYC Documents.		

26.	The solution should be able to generate the AOF and able to send as an e-mail attachment to the branch concerned. The AOF should contain the customer information, photograph captured during the interaction, OVD images and the details of agents with remarks.		
27.	The solution should have Role based access for all users such as Branch/ Admin/ Auditors/ Agents etc.		
28.	All the activity log along with the credentials of the official performing the activities shall be preserved.		
29.	Solution must support the capability to redact or black out the Aadhaar Number/Other PII in the stored video. Solution should mask the PII while displaying in DB and Video Recording.		
30.	Develop any custom MIS reports as per the requirement of our Bank with various filters.		
31.	The software should have real-time analytics of various metrics such as: Agent Rejections & Acceptance Audit rejections & Acceptance Pending at Auditor level Schedules Pending		
32.	The reports generated should be downloadable / exportable in Human readable format like Excel, pdf, csv, text etc.		
33.	Internal Dashboard to admin users for API status: Internal web portal is required for admin users which provide information for each application related to API audit logs for each API like API request, Response, status of API failure /success.		
34.	The solution should be compliant with all latest guideline of the regulatory authorities. During the contract period, successful vendor needs to make necessary changes in the solution to meet regulatory requirement changes at no additional cost to the Bank.		

35.	The bidder should ensure that all the regulations of Information Technology Act, 2000 as amended from time to time, are being adhered to.		
36.	Regular compliance of audit points raised/observed during internal audits and external audits of the application without any additional cost to the Bank within the prescribed timelines decided by the Bank.		
37.	The solution must undergo software and security audit (code audit by CERT-in empaneled auditor, RBI and any other regulators, VAPT audit in the bank end, etc.) as per stipulations and all remarks / observations in the audit reports to be rectified / incorporated.		
38.	Bank reserves right to conduct audits on the system provided by the bidder. Bidder to provide necessary arrangement and access control for the Bank.		
39.	Bidder should maintain and support its software and subsequent updates, upgrades and bug fixes such that the software remains updated and secured from vulnerabilities.		
40.	The solution should be device compatible and platform agnostic. Responsive web pages for friendly display in Desktop / mobile devices/ TAB		
41.	Security events, audit trails for all events and logs should be available for administrators and user activity should be enabled to monitor and detect suspicious activity.		
42.	The system shall maintain a log of failed and successful attempts to logon to the system.		
43.	Should comply with data retention and destruction schedules/ Policy provided by Bank.		
44.	Perform regular backup and recovery tests.		

45.	To provide Forensic Investigation Support as and when required by the Bank.		
46.	Application should restrict upload to specific types of files extensions, file size and content type.		
47.	Application should demonstrate sufficient protection against redirection flaws. Application should protect against click jacking.		
48.	Robust data backup, recovery and storability procedures with offsite and onsite backup		
49.	Application makes use of available security protocols (e.g. HTTPS, SFTP/FTPS, LDAPS, SSH, etc.) to protect sensitive data during transmission over private and public networks.		
50.	Application uses encryption (or equivalent controls such as hashing) to ensure the confidentiality and integrity of user password in storage. This involves usage of encryption technologies that have been thoroughly and publicly tested (e.g. 128-bit key length for symmetric encryption).		
51.	The Solution should be deployable on Cloud native architecture with the adaptability to the on demand up-scaling and down-scaling and seamless failover movements of the instances.		
52.	The system should have proper business continuity plan. As part of BCP, the system should be implemented at Bank's data center and disaster recovery center.		
53.	The solution should be available on High availability at DC and DR.		
54.	The bidder should provide training for selected officials. A detailed curriculum should be planned for this training program in consultation with Bank.		
55.	On the job training shall be given for Bank Officials of the Bank at Bank's Premises.		

56.	Should support compression of data with precaution that quality of images and data should not be deteriorate and decompressed after storing at Bank end if required to facilitate faster data transfer.		
57.	The application should lock the session after a specified number of authentication failures.		
58.	Provide ability for administrators to archive and backup content using one Web-based user interface.		
59.	User names and passwords must be hashed or encrypted at storage as well as before passing them over the network for authentication purpose. Hashing should confirm to at least SHA256 and above + Salt		
60.	Should support at least AES 256-bit encryption and above between web browser & web server front end (Internet & Intranet)		
61.	Proposed system should be able to disable the copy/paste and screen capture capabilities		
62.	Solution and Exposed APIs must adhere to Information Security (IS) requirement/policy of the bank/RBI's security requirements.		
63.	Solution must adhere to Data localization norms and privacy protection norms as per our bank's Statutory and Regulatory requirements		
64.	The proposed DKYC application should be compatible with and functional on the Hardware infrastructure and Operating System provided by Bank.		

Annexure 30: Technical Specifications

The bidders should provide their response against each of the Technical Specifications as per the details mentioned in the table below. Technical Specifications which are not available should be customized as per Bank's requirement without any additional cost.

Availability of the feature	Marks per feature
Available	1
Not Available	0

Module	Sub-modules	No of Requirements
Architecture & Performance	1. Architecture	25
	2. API enabled	03
	3. Backup & Recovery	10
	4. Integration	10
	5. Logging	14
	6. Performance	06
	7. Solution Design	21
Information Security	8. Information Security	52
Administrative Support & Monitoring	9. Administrative Support & Monitoring	14
Enabling features	10. Alerts & Notifications	06
	11. Master Data Management	11
	12. MIS Reports, Query and Reporting	25
	13. User Management	14
	14. Workflow	03
	Total	214

The Above Marks shall be normalized to 50 using the formula below:

$$\text{Normalized Marks} = \frac{\text{Marks Scored}}{\text{Total Marks}} \times 50$$

Module 1: Architecture

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
1.1	Solution should have a modular design enabling addition of new channels or product lines, functionally scalable, flexible architecture. The application should be built preferably on micro-services architecture with API / message based inter module integration to support selective scalability, component level deployments and upgrades.		
1.2	System to support minimum three tier architecture- Web server, App server and Database etc.		
1.3	System should be able to comply with existing regulatory authority (RBI/IBA/SEBI/Government/etc.) requirements as well as flexible to handle future such requirements that may get published.		
1.4	System should be highly parameterized to support the implementation of the bank's policy requirements and statutory policy requirements e.g., Future changes proposed by the monetary authority about timings of process, limit of process, normalization etc.		
1.5	Solution with its all components must be deployed as per Bank's requirement at all existing and future Data Centers, including but not limited to DC and DR. The solution should be deployed with high availability for DC and DR site. The High Availability architecture may span across multiple Data Centers. Solution should support DC and DR to be run in active-active mode if required.		
1.6	Solution should have modular design enabling addition of new channels or product lines or loosely coupled architecture based on micro-services pattern to provide flexibility in terms of quick feature/functionality releases and reduced time to go live.		
1.7	System should support fault tolerant architecture with respect to software, hardware, network, etc. to prevent crash of system leading to its unavailability.		
1.8	Solution Architecture should be flexible to enable customization or new feature/functionality development that are specific to the Bank.		
1.9	Solution must be highly configurable and must provide capability for the Bank to configure products and workflows which can be bundled into packages and deployed.		
1.10	The solution must handle a minimum of 100 TPS (Transactions per second).		

1.11	Solution should be designed for Cloud Native architecture to be deployed on premises at Bank's DC & DR. Solution should support containerized deployment.		
1.12	Solution should be deployed on Bank provided RedHat Open-shift container platform and RHEL VMs based on IBM S390X architecture.		
1.13	Solution should provide or support Cache services		
1.14	Solution should provide or support Queue services		
1.15	Solution should provide or support Auto scaling		
1.16	Solution should provide or support Load Balancing services		
1.17	Solution should provide or support API / Call Throttling		
1.18	Solution should provide or support Batch processing		
1.19	Solution should provide or support Message routing & transformation		
1.20	Solution should provide or support Integration with API Gateway		
1.21	Solution should preferably provide a Low-code No-Code platform to enable Bank IT team to introduce features and functionality for various journeys without the need to code.		
1.22	Solution should support horizontal and vertical scalability.		
1.23	Flexible architecture that is easy to configure, change and integrate into Bank's IT ecosystem. New functionalities should be added without impacting existing configuration & integrations.		
1.24	Solution should have a parameter-driven product and workflow configuration to onboard new products with minimal code changes.		
1.25	Solution should have a support for future integration with AI/ML-based modules (e.g., advanced fraud detection, customer segmentation).		

Module 2: API Enabled

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
2.1	Comprehensive APIs for integrating with CBS or any other system for fetching/ updating information on real time basis.		
2.2	Access to developer portal of vendor should be provided to bank to enable basic customizations/ tweaking of the available APIs.		
2.3	Parameters of API should be configurable, means ability to tweak API based on Bank's requirements.		

Module 3: Backup & Recovery

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
3.1	The system should allow having a day-end back-up process.		
3.2	The system should also have recovery features in case of system failures.		
3.3	Backup should be possible in external media tapes for off-site storage.		
3.4	Online Backup and Real time replication of data should be available between DC and DR site. Databases at all data center sites should be in sync.		
3.5	The Data replication should happen from Primary site to all DR sites on real time to keep them synchronized. In case of Solution running from DR the data replication should happen from DR site to DC on real time basis. Expected performance metrics in case of disaster: RTO (Real Time Objective): 2 hours, RPO : Near Zero		
3.6	The solution proposed should ensure regular backup on both online and offsite locations as decided by Bank. Backups taken must be periodically tested via recovery option to ensure prevention of loss of data.		
3.7	Restoration testing from back up media and DR drills to be performed every quarter as per Banks Schedule.		
3.8	Backups taken in offsite location must be preserved in a secured location with access only to bank's authorised personnel.		

3.9	No data would be purged. Server Data: All files and logs to be kept as per bank policy. Option for Archival & Purging should be available. Archived data should be made available through Bank's Object Storage and tapes.		
3.10	System should support automated archival of data as per bank policy. System should support recovery of archived data for audit or investigation purpose.		

Module 4: Integration

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
4.1	Solution should allow for Integration with CBoI internal and 3rd party external systems etc. via Industry standard approaches like Custom Adapters, RESTful API, etc. These integrations can be a) allowing access to DKYC & VKYC APIs or b) DKYC & VKYC making calls to these systems. Key aspect of all functionalities to be supported on Mobile App and need to be available through RESTful APIs with JSON.		
4.2	System should support data exchange with all the channels i.e. web upload, email, SFTP, H2H, web service /API, form based, Bulk and batch process for file transfer and future technologies channels etc. should be able to segregate different modes of processing as per the defined data.		
4.3	As part of file handling, System should be able to split /generate/control the file, in case of manual upload to desired limit as per user's requirement.		
4.4	System should be capable to Integrate with third party APIs		
4.5	System should integrate with Banks's mail systems to generate notification on mails and SMS and through auto mailers.		
4.6	System should integrate with Payment gateways for the initial deposit collections.		
4.7	System should integrate with Bank downstream systems like CBS, Omnichannel App , Digital lending platform etc.		
4.8	System should integrate with Bank's internal systems like ADS (Employee SSO), Monitoring Applications, SIEM, DAM, SOC, PIMS, Data Warehouse, DLP, Antivirus, APM, Application Whitelisting etc.		

4.9	Application should integrate with other applications like existing gateways of RBI, IDRBT, NPCI, GST, FinTech's, ONDC etc.		
4.10	Solution should host APIs viz. API (REST-Bulk) API (REST-RealTime) API (SOAP-Bulk IDOC PEXR2002 format) API (File Upload)		

Module 5: Logging

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
5.1	The system should generate error which should be descriptive enough to allow traceability of the data/function error to the most granular level as per Bank's policy.		
5.2	System should allow configuration-based start/stop of logs based on levels (Information/Warning/Error/etc.). These should be descriptive enough to allow traceability of the data/function error to the most granular		
5.3	Confidential or PII (Personally Identifiable Information) data in log should be adequately encrypted, tokenized, masked as per Bank's policy.		
5.4	Solution should provide comprehensive configuration-based event logging for monitoring, auditing and troubleshooting purposes as per Bank's policy.		
5.5	All logs should be maintained for each action taken with timestamp, unique ID, user ID, Trace ID and IP address		
5.6	Audit Logs for all Upstream & Downstream systems should be maintained as per Bank's policy.		
5.7	Audit trail for actions performed by information security administrators (at security module level) as per Bank's policy.		
5.8	Logs for any modification done should be available with the required details for audit as per Bank's policy.		
5.9	Audit trails should contain sufficient details to reconstruct events to determine the cause of the security violation or malfunction as per Bank's policy.		
5.10	Application should not allow any amendments/deletion to Audit Trails, Transaction Journal and Logs.		
5.11	Logs should be maintained at every level of the application layers as per Bank's policy.		
5.12	User related activities including successful and unsuccessful attempts to sign in must be recorded in the log files.		

5.13	Audit trails should be recorded for all activities including financial and non-financial activities at application level, DB level, Middleware level, OS level etc.		
5.14	Application logs to be integrated with Security Operations Center (SOC) for monitoring purposes as per format defined by SOC.		

Module 6: Performance

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
6.1	System Uptime should be minimum 99.95% per day.		
6.2	For the web application the static page load time (e.g., Login page) : < 2 secs		
6.3	Rendering Search results on the web pages should be < 5 seconds		
6.4	Rendering MIS reports or Dashboard should be <5 seconds.		
6.5	Application Programming Interface (API) response time should be: Asynchronous API Calls < 2 seconds. Synchronous API Calls < 1 second. These are APIs that are built and hosted by the Platform.		
6.6	Transaction failure due to technical reasons below 0.01%		

Module 7: Solution Design

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
7.1	Access to application API from Corporate/Government would be via secure authentication e.g. TLS, Encryption, Digital Signature, Tokenization etc. As per Bank's policy guidelines time to time without any development / additional cost to the bank.		
7.2	Solution should be Web Application compatible on all latest versions of major web browsers- Microsoft Edge, Google Chrome, Mozilla Firefox, Safari etc. and on mobile application without any development / additional cost to the bank.		
7.3	Web applications to be built are DKYC, VKYC, PLC & ReKYC		

7.4	The solution interface should support adaptive design based on various form factors available in Desktops, Laptops, Smartphones, Tablets, etc. which would be used by the end users of this application as per Bank's design guidelines.		
7.5	Solution would have web portal-role based access for Bank Users: Super Admin, Admin, Marketing Executives, RMs, Central Office users, Branch Maker, Branch Checker, MIS/Report User etc. Agents: B) VKYC Handling agents. C) VKYC Auditors D) DKYC Makers E) DKYC Checkers The application and workflow should be customized as per Bank's requirement.		
7.6	The system should generate standard custom defined error messages based on pre – defined parameters.		
7.7	End-users would see business friendly messages while the actual error message should be made available to IT team for Root Cause Analysis (RCA) purposes.		
7.8	Solution should have Bank's branding in terms of logo, color schemes, fonts and other branding content on the channel etc. as per Bank's design guidelines		
7.9	The system should be capable of displaying the details of corporate, Government body's logo, name, address on the portal as part of personalization.		
7.10	It should support data entry via upload of files in various industry specific standard formats like ZIP, RAR, PDF, XML, IMAGES (JPG,JPEG, TIFF, etc.), EXCEL, DOC(x), TXT (Delimited & Fixed length), CSV, DAT, ISO 20022 etc. centrally or from Corporate/Government/banks location etc.		
7.11	System should support file formats with headers, footers and blank lines or without headers, Footers and blank lines, with any delimiter as required by clients		
7.12	It should support ISO8583 messaging formats etc.		
7.13	System should have user-friendly and intuitive interface as per Bank's design guidelines		
7.14	Access to the solution for Banks employees should be from Banks Intranet / VPN / MDM, TAB, Mobile devices.		
7.15	For devices to be used for access by Bank Employees (via Intranet access), Solution should support Office connected desktop/Laptop, TAB, Mobile, MDM connected devices etc.		

7.16	For devices to be used for access by Corporate/Govt. users. (Via Internet Access.), Solution should support Desktop/Laptops/Smartphones from Internet or via VPN access. Additionally, access via H2H / SFTP /API/ Dedicated connections/etc. also must be provided. The Architecture design should support them.		
7.17	Version Control and rollback Mechanism should be implemented to track both product versioning as well as the custom design that gets released to production. Solution should integrate with Bank's DevSecOps platform for Versioning and CI/CD deployment, Project Management, Container Registry and Security Scans.		
7.18	Proposed solution should have integration with Bank's Omni-channel Platform.		
7.19	System should ensure processing of unique transactions only so that no transactions are processed twice.		
7.20	The system should be capable of displaying advertisement and marketing banners on the portal - On login page and on landing page post login.		
7.21	Solution should have file Format Mapper - Ability to define & map file formats (input file as well as response file) as per customer's unique requirements.		

Module 8: Information Security

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
8.1	Secure coding practices should be used. Please refer NIST SP 800-204C or the latest one for detailed guidelines on Microservice based architecture		
8.2	NIST SP-800-190 (Application Container Security Guide) should be followed for Microservice based architecture		
8.3	If source code is not shared with bank, then Vendor to provide latest Security Review Report done by any CERT-IN empaneled ISSP		
8.4	Application should be tested and patched against known vulnerabilities as defined in OWASP Top 10 and SANS 25 prior to handover to the Bank.		
8.5	No static details regarding project (e.g., Default username, password) are mentioned in the code.		
8.6	Obfuscation of code to be done while putting the project into production.		
8.7	DevSecOps activities and processes should be followed and aligned with SDLC (Software Development Lifecycle) framework in Agile mode and IT service management processes (e.g., Configuration management, change management, software release management). Bank's DevSecOps platform should be used for the above activities.		
8.8	Transfer of software from development to test and test to production should follow a controlled procedure to ensure that only the software that has undergone testing can be released to production. Bank's DevSecOps platform should be used for the activities.		
8.9	Adequate knowledge transfer should be planned. Knowledge transfer includes but not limited to transfer of skills, operating processes, and procedures. Focused training sessions, handholding for certain period and detailed documentation should be used to ensure knowledge transfer. Reverse Transition Plan should be made available.		
8.10	Vendor to support DevSecOps Implementation using Bank's DevSecOps Platform to ensure that Deployment/Rollback in production would be automated without the need for access to servers for Vendor.		
8.11	The software solution should follow best practices in architecture, design and coding. In the case of web application, it must adhere to OWASP design and security guidelines.		

8.12	System should support Single Sign-On (SSO). Single Sign-On would have to be with the Active Directory Services (for Employees). Single login and single reference ID (corporate ID) for all modules and single sign on Omni-Channel.		
8.13	The PII data should be stored encrypted form. It should have capability for data encryption, tokenization and masking. Movement should also happen in encrypted form.		
8.14	The data should be stored in encrypted form as per Bank's policy.		
8.15	Movement of data should also happen in encrypted form as per Bank's policy.		
8.16	Solution should have capability for data masking, encryption, tokenization and data vaulting etc..		
8.17	Users should be able to change their passwords for login/ transactions without manual intervention. This process must be secure with Multi- Factor Authentication (MFA)		
8.18	Bank users would follow the existing policy on password changes as it would be integrated with their employee account in Active Directory.		
8.19	Support two/multi factor authentication mechanism during login e.g. OTP, Biometric , Tokens /Soft Token/Hard token or any other secure way of login		
8.20	All credentials regarding the application solutions like Application, Database, OS passwords etc should rest with Banks Authorised personnels only. Role based access to the system should be available.		
8.21	System should be deployable on secured and hardened infrastructure including Application, OS, Database, load balancers, middleware (e.g. web servers Tomcat, WebSphere etc.) as per Bank's policy		
8.22	System to support Virtual keyboard option during password entry during corporate login.		
8.23	The Unsuccessful attempts to log-in to the system should be recorded on the log files.		
8.24	Verification of identity of users through User Id/ Passwords (As per banks password policy & in encrypted format).		
8.25	Solution should support Mechanism of Multifactor Authentication of Transaction Authorization – OTP, Biometric, Transaction password, Tokens /Soft Token/Hard token, or any other secure way of authorizing transactions		
8.26	It should check/record/verify authentication of source of each transaction like user IDs, IP address, Mac address etc. and maintain logs which is required for AUDIT purpose.		
8.27	Data entry / upload of files should be with due authentication and encryption		

8.28	Support for file upload with digital signature/ RSA token/ encryption.		
8.29	Option for Two or more users should authorize file upload, with provision for multi- level authorization for bulk/individual uploads depending on Bank's requirement (e.g., Multilevel authorization for amount exceeding a ceiling limit). Maker checker concept should be present.		
8.30	System should support forgot password retrieving facility.		
8.31	System should support inactivity period number or retries for login feature, last login time, session time, out time, idle time etc. as per Banks policy.		
8.32	System should support CAPTCHA authentication.		
8.33	Movement of data (in Transit) should be secured and encrypted via TLS 1.2 and above		
8.34	System should support security features such as SFTP, HTTPS, Digital Certificates etc.		
8.35	System should support security features such as encryption, decryption, hashing, salting, signature verification etc.		
8.36	System should support security features such as digitally signed data transmission and verification.		
8.37	Different levels of authorization should be available. System should be capable to allow users to access /create/ modify object or functionality as per their roles.		
8.38	System should support TLS1.2 and above certificate and as per Bank's policy on time to time		
8.39	System should adhere to any data related requirement as prescribed by the regulator, government or Bank from time to time. This adherence should not result in any cost impact to the bank.		
8.40	System should have auto log-off functionality on session timeout or user inactivity, idle timeout etc. as prescribed by the Banks IS policy.		
8.41	The solution should provide H2H integration with encryption, decryption and digital signature with corporate ERP/ other operating systems for secure file transfer between the corporates and the Bank. Encryption algorithm of client should be supported by the system.		
8.42	Architecture should ensure the security of the deployment architecture by segregating the servers into various security zones, e.g. Web Server in DMZ, App Server in MZ, Database in Core MZ, etc.		
8.43	Any type of Remote access to the system outside the Bank's network will not be allowed.		

8.44	Proposed Solution should integrate with Bank's existing Aadhar Vault to store and retrieve Aadhar Numbers.		
8.45	Open source software components will not be considered in the solution. All components should be with enterprise license and highest level /Grade of 24X7OEM support. For the entire contract period of 5 years. The software should be supplied with enterprise license only. Community edition/open licenses will not be accepted by the Bank.		
8.46	System should support IPv4 & IPv6 protocols.		
8.47	Data at Rest: Application Logs: To be encrypted. PII (Personally Identifiable Information) data should be masked. Log structure should be as per CBOI guidelines. Database: TDE (Transparent Data Encryption) & Redaction to be implemented, PII Data stored in Database should be in encrypted format, encryption and decryption should be taken care by the application in real time. All passwords/PINs: should be hashed with Random salt at the time of input. Minimum: SHA-2 or equivalent and above		
8.48	<u>Data in Transit:</u> Channel level security TLS 1.2 and above in all communications including Web to App to DB server. All File based communication to have additional encryption on file. API communication should have payload encryption in additional to authenticated access. No sensitive/PII data should be visible/in plain text during the whole communication including internal communications.		
8.49	API Integration: Authentication: Token based, Symmetric/Asymmetric encryption, hashing Payload: Payload Encryption.		
8.50	Application should support Bank's Password policy. The solution must be integrated with Bank's Active Directory using LDAP.		
8.51	Access of the solution for other systems (Internal/external) would be via authenticated and secure API calls.		
8.52	Access to the infrastructure hosting the solution would be via restricted, authenticated access through Privileged Identity Manager. This access would be available only from the Bank's IT Centers and on Bank Network. Test, Pre-prod environment: Access to Vendor and Bank IT		

	teams. Production (and DR): Access would be given to Access to Vendor Support team and Bank IT Teams		
--	--	--	--

Module 9: Administrative Support and Monitoring

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
9.1	System should have facility for monitoring all files & transactions for customers and Ops team. The system should be monitorable at component level and required telemetry (observability), logs available for quick response & resolution in defined SLAs.		
9.2	Community editions of any components are not allowed even if supported by the bidder.		
9.3	User administration Module for managing user accounts, defining roles and rules, workflow, Monitoring of user activities.		

9.4	Define workflow for various system activities through setting parameters through front end.		
9.5	Managing and Monitoring of system resources like storage, usage and likewise.		
9.6	Version maintenance, change management and tracking of Application, Scheduling back up of application.		
9.7	Maintenance of UAT environment. UAT set up should be in synchronization with live application in terms of Database structure and functionality.		
9.8	Module for tracking change requests.		
9.9	Audit trails should be enabled for all activities including financial and non-financial activities.		
9.10	Logs for all/any modification done should be available with the required details for audit.		
9.11	Audit trails should contain sufficient details to reconstruct events to determine the cause of the security violation or malfunction.		
9.12	Application should not allow amendments/ deletion to Audit Trails, Transaction Journal and Logs.		

9.13	The application should have the master maintenance module along with the owner (creator, verifier, checker, administrator and viewer role).		
9.14	The bidder should provide a mechanism to monitor the Database.		

Module 10: Alerts & Notification

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
10.1	System should be able to provide internal notification for action item, pending authorization, final authorization to authorized users/approvers etc.		
10.2	System should support notification through various modes such as email, SMS etc. automatically as per banks requirements. This notification can be to internal (bank) or external (Customer/Agency/etc.) users etc.		
10.3	System should support E-mail and SMS alerts for Exceptions.		
10.4	System should be able to integrate with Bank's downstream applications like Core Banking Solution, Integrated Payment Hub (IPH), Executive Information System (EIS), Bank's API Gateway, APM tool, Aadhaar Data Vault (ADV), Enterprise Service Bus (ESB) etc. on real time basis to pull data for giving alerts/ notifications		
10.5	Alerts on specific transactions based on events. This should be customizable and should not require code level changes and redeployment. (e.g., broadcasting message for shift to DR)		
10.6	Alerts (SMS & email) & notifications on transactions, creation, renewals, inactive customers etc.		

Module 11: Master Data Management

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
--------	------------------------	----------------------	---------

11.1	System should have Master Data Management module with Maker-Checker functionality and audit trail around it.		
11.2	System should be having functionality for creating and maintaining Customer/ Bank/Branch and any other Masters (Data entry and File upload system etc.).		
11.3	Master Data module should be loosely coupled with the system so that any additions/updates to master data need not require solution redeployment		
11.4	System should be capable of defining the charges at client level/product level at various frequencies like monthly/quarterly/yearly etc.		
11.5	System should have ability to define holidays, day begin and day end facility. System should be capable of maintaining Holiday masters: national / state / district / branch / day wise.		
11.6	Capability for client master creation with all KYC compliance. System should be capable of maintaining client wise authorization / escalation matrix.		
11.7	Customer master should support single account, multiple account, limits for each account and charges.		
11.8	System should have the ability to bulk upload for creating Users, Group creations, Authorization mappings, maintain list, create rules, Account linking etc.		
11.9	System should have bulk uploading functionality to upload customers data files like LEI master etc. with modification / deletion or addition etc.		
11.10	System should have the ability for modification/addition of multiple accounts in existing group at one go.		
11.11	The DKYC & VKYC should be able to maintain or fetch master data from CBS or through any upload. The following master shall be maintained: h) Bank and Branch masters (through manual entry/file uploading) along with location master i) Account, Product master j) Authorization and Escalation matrix k) User master l) User role definition master with upgrade and downgrade of user		

	m) Holiday master's maintenance (national / state / district / branch / day wise) for admin users. n) o) Product set up parameters should be configurable through front end.		
--	---	--	--

Module 12: MIS, Query and Reporting

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
12.1	System should support schedule-based generation and mailing of various reports through scheduler and auto mailer as per banks requirement.		
12.2	Allow users to export MIS reports in standard formats like Excel, PDF, TXT, CSV, XML, JSON etc.		
12.3	System should have facility to enable Bank to login and download MIS reports required by them over WEB, API, Email, SFTP, H2H etc.		
12.4	The system should allow users to download and print reports directly from their login.		
12.5	There should be provision to send variety of reports through AUTO MAILER and on required frequencies		
12.6	Provision to send similar type of reports to specific group through auto mailer. Parameterization required for selection of auto mailer reports.		
12.7	Exception reports should be available.		
12.8	Application should have basic reporting options and should have report building flexibility to users. Facility to design reports as per requirements. Report writer/builder should be available to the Bank to generate their own reports and queries.		
12.9	System should support various hierarchy-based reports like Branch manager should have access to his branch report and Regional Office, Zonal Office, Central Office have access to overall reports etc. rule and role based.		

12.10	Interface with Drag & Drop/mapping of fields option to create dynamic MIS formats based on the requirements from different clients. Since requirements will be different from client to client, defining of MIS formats can be easy for various requirements from clients.		
12.11	System should provide separate, incremental, cumulative, consolidated MIS etc. for collection as well as payments in the format required by client.		
12.12	MIS Module should support all latest security algorithms like Digital Signature, PGP etc. for encryption and decryption of files.		
12.13	MIS reports can be viewed across various devices like mobile, laptop, desktops and tablets.		
12.14	MIS and databases should be readable via third party tools like Tableau, R, Power BI, Python, SQL Developer etc. and exportable in csv, txt, xml etc. formats for running analytics.		
12.15	MIS and Real time reports generation should be possible from DR servers.		
12.16	System should enable monitoring of all transactions and files both at bank end. System should support monitoring of processing engines and related integrations		
12.17	The application should be integrated to Bank's mail server & SMS server for sending the generated MIS through auto mailers / auto SMS.		
12.18	The application should be configurable to fetch data from various platforms through API for generation of various reports.		
12.19	The files generated from DKYC & VKYC application in the form of MIS reports should be non-tamperable within the Bank and at client end.		
12.20	Application should have basic querying options and need to be customized based on the products/ processes defined by the Bank.		
12.21	Application should provide multiple initiation modes, query for areas including real time status, real time alerts and notifications and download reports.		
12.22	Application should have basic reporting options and should have report building flexibility to users.		

12.23	It should have the facility to design the reports as per the Bank's requirements.		
12.24	System should enable the user to view the full details of a customer. Account aggregation – one view account summary of all accounts in a single or multiple report.		
12.25	The notifications must be customizable by the Corporate as follows – d) Text of the message e) Incorporate variable data from DKYC & VKYC transaction tables Channel for delivery - email, SMS or WhatsApp, as required		

Module 13: User Management

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
13.1	User Management Module to be available for Bank. With audit trail capability.		
13.2	Role based access to be supported for customers which should be configurable.		
13.3	Addition/ management/ activation/ deactivation/ reactivation/ modification/ deletion of user profiles- internal roles (bank) and external roles (customers)		
13.4	Bank can administer and manage user creation and profiles, roles and workflow rules for their respective entity.		
13.5	Multi users with granular access controls/ entitlements and work flow management		
13.6	User management options like lock, unlock, reset login password etc.)		
13.7	Support organization hierarchy, user, role based access with proper authentication and audit trails		
13.8	System should provide features for disabling a user, temporarily suspending rights to a user and automatic deactivation of user in case of inactivity for a defined period.		
13.9	System should have the ability to upgrade and downgrade the user.		

13.10	System should have the ability to import currently onboarded data/old data of customers.		
13.11	User administration Module for managing user accounts, user groups, Defining roles and rules, approval workflow and monitoring of user activities.		
13.12	System to identify user type basis login credentials and route to respective landing page (maker, checker, authorizer)		
13.13	Authorized users to perform transactions on the selected account up to the specified transaction limit		
13.14	User management and access rights configurations should be supported by way of individual users or group of users for records or file uploads		

Module 14: Workflow

Sr No.	Technical Requirements	Available (YES / NO)	Remarks
14.1	Define workflow for various system activities through setting of parameters through front end.		
14.2	System should have a workflow which provides flexibility of Multi- level/ Sequential/ Parallel/ Quorum based approval workflow rule definition. These should be configuration based.		
14.3	Bank Users should be able to define workflow, queues and priorities based on various criteria, such as queue for items needing manual intervention with proper notification, if item in queue is awaiting or exception has occurred		

Annexure 31: Board Resolution

CERTIFIED TRUE COPY OF THE RESOLUTION PASSED AT THE MEETING OF THE BOARD OF DIRECTORS OF (Company Name) _____ HELD ON (Board Resolution Date) _____ AT (Venue/Registered Office Address) _____

1. **RESOLVED THAT** the Company be and is hereby authorized to participate in the tender/RFP invited by **Central bank of India** to procure Supply, Procurement, Implementation and Maintenance of Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels as provided RFP titled "[Insert Tender/RFP Title/Reference Number]"
2. **RESOLVED FURTHER THAT** [.....Name of Director/Employee], [.....Designation] [.....DIN No.] of the company, be and is hereby authorized to:

To do all the necessary steps including and not limited to registering the / enrolling e- platform, authorized to sign and submit all the necessary papers, letters, forms, etc. to be submitted by the company in connection with the above RFP and its subsequent processes. The acts done and documents shall be binding on the company, until the same is withdrawn by giving written notice thereof to Central bank of India in time. Authorized to **Sign, seal, and submit** the bid documents, technical proposal, and financial proposal (RFP/Tender), **Execute Performance Bank Guarantee /bonds, and indemnities and other Service Level Agreements, Pay Earnest Money Deposit (EMD)** and Tender Fees, as necessary required for the tender process also do all acts/ take necessary steps for all ancillary and incidental in this regard.

3. **RESOLVED FURTHER THAT** all acts, deeds, and things done by the said Authorized Signatory, in connection with the above-mentioned tender, shall be binding on the Company.

4. **RESOLVED FURTHER THAT** a certified true copy of this resolution along with the specimen signature of the Authorised signatory be submitted to the concerned authority/agency, and they be requested to act thereon.

Signature /-
True copy

(to be signed by **Company secretary or Managing Director** with name and specific designation and date and place)

Specimen signature of the **Authorised Signatory**:

Detail of OVD of Authorised signatory : Adhaar / Voter ID/DL etc No

Signature /-
True copy

(to be signed by **(to be signed by Company secretary or Managing Director with name and specific designation and date and place)**
with name and specific designation and date and place)

*Should Print on Letter head of the company and should put page number.

Annexure 32: Format for Submission of Client References by Bidder.

To,

Asst. General Manager-IT
Central Bank of India
Cent Neo, 6th Floor, Tower No.7
Belapur Railway Station Complex, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sub: RFP for Procurement, Implementation and Maintenance of On-Premises Solution for Customer On-boarding through DIGITAL KYC, VIDEO KYC and other channels

Particular	Details
Client Information	
Client Names	
Client Address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
• Name of the Project	
• Description of the project	
• Implementation Start Date	
• Implementation End Date	
• Support & Maintenance Start Date	
• Support & Maintenance End Date	
Current Status (In Progress / Completed)	
Size of Project	
Number of Customers being addressed through the Project	
Any other information on the Client Reference	

The documentary proof of the client reference is enclosed.

Yours faithfully,

Signature of Authorized Signatory:

Name of Signatory:

Designation's

Seal of Company:

Date:

Place:

16. Checklist For Submission:

No.	Particulars	Bidders Remark (Yes/No)
1	Certificate of Incorporation	
2	Undertaking / Power of Attorney (PoA)	
3	Audited Balance sheets of last three years - 2022-23, 2023-24, 2024-25	
4	CA certificate for three years average turnover for financial years 2022-23, 2023-24, 2024-25	
5	CA certificate for operating profit for last three financial years 2022-23, 2023-24, 2024-25	
6	CA certificate for net worth for last three financial years i.e. 2022-23, 2023-24, 2024-25	
7	Copy of the Purchase Order and Work Completion Certificate	
8	Self-declaration by the Authorized Signatory for not having filed for Bankruptcy in any country including India on company letter head	
9	Self-declaration on Company's letter head stating that the bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks	
10	Self-declaration on Company's letter head stating that the service provider has no legal proceedings / Inquiries / investigations have been commenced / pending / threatened against service provider by any statutory or regulatory or investigative agencies for which performance under the contract will get adversely affected / may get affected.	
11	Self declaration on Companys letter head stating that Bidder under notice/termination period from OEM/OSD as on bid submission date should not bid in this tender.	
12	Supporting Document ensures that the Bidder is certified with any one certificates among CMM Level 3 or above, ISO 27001, SOC2. (valid during the RFP process).	
13	Copy of the registration certificate signed by authorized signatory	
14	Self-declaration on Company's letter head regarding • NPA • Any case pending	
15	Self-declaration on Company's letter head that the Bidder, is not owned or controlled by any director or key officer/employee of the Bank or their relatives having the same meaning as assigned under Companies Act, 2013 and the rules framed thereunder, as amended from time to time	

16	Reference letter confirmation from the BFSI Organization that the solution is implemented & running. It should be signed (along with BFSI Organization seal) not below the Rank of CM (Scale- IV or equivalent)	
17	Copies of MOA/AOA	
18	Copies of shareholding pattern	
19	PAN, TAN, GSTIN Certificate, MSME Registration Certificate (If Applicable) and any other tax related document if applicable is required to be submitted along with the eligibility bid.	
20	Declaration supported by documentary evidence (CA Certificate) for no employees	
21	Undertaking along with Annexure-29 should be submitted for compliance to functional specifications mentioned in annexure 29	
22	Undertaking along with Annexure-30 should be submitted for compliance to technical specifications mentioned in annexure 30	
23	Annexure 1: Conformity Letter	
24	Annexure 2: Compliance to Terms & Conditions	
25	Annexure 3: Pro-forma for deed of indemnity	
26	Annexure 4: Undertaking of Authenticity for Products Supplied	
27	Annexure 5: Undertaking for Acceptance of Terms of RFP	
28	Annexure 6: Manufacturer's / OSD Authorization Form	
29	Annexure 7: Pre- Contract Integrity Pact	
30	Annexure 8: Non-Disclosure Agreement	
31	Annexure 9: Performance Bank Guarantee (PBG)	
32	Annexure 10: Pro-forma for Bid Security (EMD)	
33	Annexure 11: Letter for Refund of EMD	
34	Annexure 12: NPA Undertaking	
35	Annexure 13: Undertaking letter - Land Border Sharing	
36	Annexure 14: List of Hardware and Software Components	
37	Annexure 15: Cover Letter	
38	Annexure 16: Bidder's Particulars on Company Letter Head	
39	Annexure 17: Guidelines on banning of business dealing	
40	Annexure 18: Proposed Team Profile	
41	Annexure 19: Format for Submission of Client References by Bidder	
42	Annexure 20: Query Format	
43	Annexure 21: Eligibility Criteria Compliance	

44	Annexure 22: Undertaking for 5 Year Roadmap	
45	Annexure 23: Compliance to Security Control	
46	Annexure 24: Undertaking for Information Security	
47	Annexure 25: Undertaking for Data Privacy	
48	Annexure 26: Format for Local Content	
49	Annexure 27: Undertaking for Non- Blacklisting/ Non-Debarment of the bidder	
50	Annexure 28: Masked Commercial Bid	
51	Annexure 29: Functional Specifications	
52	Annexure 30: Technical Specifications	
53	Annexure 31: Board Resolution	
54	Annexure 32: Format for Submission of Client References by Bidder	

--- END OF DOCUMENT ---